ADMINISTRATION

ADMINISTRATION GÉNÉRALE

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ

MINISTÈRE DE LA COHÉSION DES TERRITOIRES

SECRÉTARIAT D'ÉTAT CHARGÉ DES PERSONNES HANDICAPÉES

Secrétariat général

Haut fonctionnaire de défense et de sécurité

Direction générale de la cohésion sociale

Service des politiques d'appui

Sous-direction de l'enfance et de la famille

Instruction n° SG/HFDS/DGCS/2017/219 du 4 juillet 2017 relative aux mesures de sécurisation dans les établissements et services sociaux et médico-sociaux

NOR : *SSAZ1720247J*

Date d'application : immédiate.

Validée par le CNP le 22 juin 2017. – Visa CNP 2017-79.

Examinée par le COMEX JSCS, le 27/06/2017.

Catégorie : directives adressées par le ministre aux services chargés de leur application, sous réserve, le cas échéant, de l'examen particulier des situations individuelles.

Résumé : la présente instruction vise à renforcer la politique de sécurité des établissements et services sociaux et médico-sociaux.

Elle précise :

– les mesures à mettre en œuvre par les établissements et services sociaux et médico-sociaux concernés,

– le rôle des agences régionales de santé (ARS) pour les établissements et services médico-sociaux et des directions régionales de la jeunesse, des sports et de la cohésion sociale (DR[D]JSCS) pour les établissements et services sociaux dans l'animation et la coordination de la politique régionale de sécurité pour le secteur social et médico-social.

Mots clés : sécurité – sûreté – plan Vigipirate – règlement de fonctionnement – fiche de sécurité – prévention des attentats – radicalisation.

Références :

Articles L.312-1, L.312-1, R.311-35, L. 349-1 et suivants du CASF ;

Circulaire du Premier ministre du 13 juin 2016 relative à la prévention de la radicalisation ;

Circulaire ministérielle n° DGCS/SD2C/2016/261 du 17 août 2016 relative à la préparation aux situations d'urgence particulière pouvant toucher la sécurité des établissements d'accueil du jeune enfant ou des établissements relevant de la protection de l'enfance ;

Instruction n° SG/2016/14 du 8 janvier 2016 relative au cadre d'intervention des agences régionales de santé s'agissant des phénomènes de radicalisation ;

Instruction DGS/DUS/SGMAS/SHFDS n° 2016-40 du 22 janvier 2016 relative aux principes d'organisation des missions de veille et de sécurité sanitaire et des missions relevant des domaines de la défense et de la sécurité au sein des agences régionales de santé ;

Instruction n° SG/HFDS/2016/340 du 4 novembre 2016 relative aux mesures de sécurisation dans les établissements de santé ;

Textes relatifs à la PGSSIS dans le secteur social et médico-social.

Annexes :

Annexe 1. – Lignes directrices pour l'élaboration d'une ligne de sécurité.

Annexe 2. – Sensibilisation et formation des professionnels.

Le ministre de la cohésion territoriale, la ministre des solidarités et de la santé et la secrétaire d'État chargée des personnes handicapées à Mesdames et Messieurs les préfets de région ; Mesdames et Messieurs les préfets de département ; Mesdames et Messieurs les directeurs généraux des agences régionales de santé ; Mesdames et Messieurs les directeurs régionaux de la jeunesse, des sports et de la cohésion sociale ; Mesdames et Messieurs les directeurs régionaux et départementaux de la jeunesse, des sports et de la cohésion sociale ; copie à : Mesdames et Messieurs les directeurs de la jeunesse, des sports et de la cohésion sociale outre-mer ; Mesdames et Messieurs les directeurs départementaux de la cohésion sociale et de la protection des populations ; Mesdames et Messieurs les directeurs départementaux de la cohésion sociale.

Les établissements et services sociaux et médico-sociaux (ESSMS) sont par nature des espaces ouverts au public, ils accueillent en permanence des usagers et leurs proches. Comme tous les organismes reçevant du public, ils peuvent se trouver confrontés à toutes les formes de violence que connait notre société.

Les responsables d'ESSMS se doivent de rechercher les moyens d'assurer dans leur enceinte la sécurité des personnes et des biens. Cet impératif concerne aussi bien les résidents/usagers, que les visiteurs, les intervenants extérieurs ou les personnels. Ces derniers peuvent en effet également se trouver confrontés à une agression, quelle qu'en soit sa gravité et son origine (responsabilité du chef d'établissement et de l'employeur art. L. 4121-1 et L. 4121-2 du code de travail).

De plus, le contexte de menace terroriste et les récents attentats imposent une vigilance accrue et nécessitent d'assurer, sur l'ensemble du territoire, la mise en œuvre effective de mesures particulières de sûreté au sein des établissements et services sociaux et médico-sociaux.

L'objectif de la présente instruction est donc de développer une politique globale de sécurité, visant à protéger les ESSMS tant contre les violences qui peuvent se produire au quotidien que contre la menace terroriste, aujourd'hui multiforme.

Les structures concernées sont les ESSMS visés au I de l'article L.312-1 du code de l'action sociale et des familles (CASF) qui, selon les termes du dernier alinéa, « assurent l'accueil à titre permanent, temporaire ou selon un mode séquentiel, à temps complet ou partiel, avec ou sans hébergement, en internat, semi-internat ou externat. », à l'exception de ceux cités aux alinéas 4° et 13°, car situés respectivement dans le champ de compétence de la Protection judiciaire de la jeunesse, et dans celui du ministère de l'Intérieur. À ces structures sont rajoutés, bien que n'étant pas des ESSMS *stricto sensu*, les centres d'hébergement d'urgence, auquels il est recommandé d'assurer la sécurité des personnes hébergées en s'inspirant des mêmes modalités que celles prescrites aux ESSMS.

Afin de décliner au niveau territorial cette politique de sécurité, cette instruction organise l'appui aux ESSMS en prescrivant l'animation et la coordination régionales par les agences régionales de santé (ARS) pour les établissements et services du secteur médico-social et par les directions régionales de la jeunesse, des sports et de la cohésion sociale (DR(D)JSCS) pour les établissements du secteur social, en étroite concertation avec les présidents de conseil départemental dans les cas de compétence conjointe.

1. Les mesures à mettre en œuvre par les établissements et services sociaux et médico-sociaux concernés

Chaque structure établira sa propre stratégie de protection en veillant à la cohérence avec les instructions gouvernementales, notamment le plan Vigipirate[1], qui fixe la réponse gouvernementale en matière de vigilance, de prévention et de protection face à la menace terroriste. Dans sa nouvelle version de décembre 2016, il vise à mieux informer les citoyens sur le terrorisme, les mécanismes déployés pour y faire face ainsi que sur les gestes et les comportements qui protègent et qui sauvent. Il s'agit ainsi d'élever la capacité de résilience de la société tout entière. Un document public, « Faire face ensemble », a été rédigé à cet effet, pour les responsables de sites accueillant du public d'une part, mais aussi pour l'ensemble de la population.

[1] La partie publique du plan Vigipirate de décembre 2016 « Faire Face Ensemble » ainsi que les logos sont téléchargeables sur : http:/www.gouvernement.fr/risques/le-citoyen-au-coeur-du-nouveau-dispositif-vigipirate.

La posture Vigipirate est adaptée périodiquement en fonction des circonstances ou des menaces particulières. Cette adaptation fait l'objet d'une note de posture du haut fonctionnaire de défense et de sécurité (HFDS) des ministères sociaux ; diffusée aux différentes administrations territoriales (préfectures, ARS, DR(D)JSCS) et à l'ensemble des établissements.

1.1. *L'actualisation du règlement de fonctionnement ou l'élaboration d'une fiche de sécurité*

L'article R.311-35 du CASF dispose que le règlement de fonctionnement des ESSMS prévu à l'article .L. 311-7 du CASF, « précise les mesures relatives à la sûreté des personnes et des biens et prévoit les mesures à prendre en cas d'urgence ou de situations exceptionnelles ».

Dans ce cadre, avant la fin de l'année 2017, chaque directeur d'ESSMS devra en fonction des spécificités de sa structure (taille, environnement, configuration des locaux, type de population prise en charge…) :

– soit actualiser son règlement de fonctionnement afin d'y intégrer les mesures de sécurité adéquates,
– soit élaborer une fiche de sécurité qui sera annexée au règlement de fonctionnement. Dans cette option, si l'ESSMS est implanté dans une autre structure (ex : établissements de santé ou école…) disposant déjà d'un plan de mise en sécurité, le directeur vérifiera que celui-ci est bien étendu à l'ESSMS, sinon il élaborera sa propre fiche de sécurité, en cohérence avec la démarche de la structure d'accueil.

Conformément à l'article L. 311-7 CASF, ces documents (règlement de fonctionnement ou fiche de sécurité en annexe au règlement) seront présentés au conseil de la vie sociale ou à la structure de participation des usagers équivalente.

Pour élaborer leur fiche de sécurité ou mettre à jour leur règlement de fonctionnement, les ESSMS pourront s'appuyer sur l'annexe n° 1 et sur les guides référencés réalisés à cet effet.

La fiche de sécurité s'appuiera sur une analyse de risques identifiant les principaux éléments de vulnérabilité. Elle comprendra deux parties distinctes :

– une partie générale, comprenant les mesures globales de sécurisation liées à la protection de la structure dans la durée et intégrant les mesures du plan Vigipirate ;
– une partie « gestion de crise », traitant des mesures particulières et immédiates de sécurité à mettre en œuvre notamment en cas de survenance d'un attentat au niveau local et de risques potentiels de sur-attentat.

Il est recommandé de réviser la fiche de sécurité annuellement.

En lien avec les services spécialisés concernés, des exercices annuels sont recommandés dans les ESSMS afin de tester le dispositif de sécurité, et de s'assurer de son appropriation par le personnel de la structure.

Pour les accompagner dans leur démarche de sécurisation de l'établissement, les directeurs des ESSMS pourront solliciter l'appui :

– des préfectures, des forces de police et de la gendarmerie (référents sûreté) ;
– des correspondants sécurité des ARS pour les établissements médico-sociaux ;
– des conseillers de défense et de sécurité de zone des agences régionales de santé ;
– des conseillers de défense et de sécurité de zone des DR(D)JSCS ;
– du ministère des affaires sociales et de la santé : service spécialisé du haut fonctionnaire de défense et de sécurité (hfds@sg.social.gouv.fr) et délégué à la sécurité générale de la direction générale de l'offre de soins (sante-securite@sante.gouv.fr).

1.2. *La prévention de la radicalisation*

La radicalisation de personnes ayant accès aux ESSMS peut mettre en danger leur sécurité. Il convient donc d'être attentif à ce phénomène et notamment de mettre en place les mesures de prévention prévues dans l'instruction aux ARS du 8 janvier 2016 et dans la circulaire du Premier ministre du 13 mai 2016. La radicalisation éventuelle de personnels de l'établissement doit également être prise en compte.

Les directeurs d'ESSMS doivent diffuser l'information au sein de leur structure sur les risques liés aux phénomènes de radicalisation. Ils devront toutefois adapter leurs propos à la catégorie de résidents ou d'usagers pour ne pas inquiéter des populations fragiles, par exemple des personnes souffrant de handicap psychique ou des personnes âgées.

Il est rappelé que le ministère de l'intérieur a édité un référentiel sur lequel l'ensemble des acteurs peut s'appuyer. Toutefois, toute personne a la possibilité de signaler des personnes en voie de radicalisation (personnel, usagers, prestataires) auprès du centre national d'assistance et de prévention de la radicalisation qui dispose d'un numéro vert : 0 800 00 56 96.

Pour les professionnels, le signalement peut se faire directement au numéro vert mais également à travers la voie hiérarchique auprès des services préfectoraux.

1.3. *La prise en compte de la sécurité des systèmes d'information*

Le développement rapide de l'usage des technologies de l'information dans le domaine du social et de la santé contribue largement à l'amélioration de la qualité des soins et du suivi des usagers et des patients. En contrepartie, il s'accompagne d'un accroissement significatif des menaces et des risques d'atteinte aux informations conservées sous forme électronique. Plus généralement, le danger concerne tout processus de santé s'appuyant sur des systèmes d'information numérique (ex circuit du médicament).

Les menaces pesant sur les systèmes d'information numérique gagnent en intensité et en sophistication et constituent un risque réel pour le fonctionnement des établissements. Ce contexte nécessite une attention particulière de la part des directeurs d'ESSMS afin d'identifier les vulnérabilités des systèmes d'information utilisés, de renforcer la vigilance des utilisateurs comme des administrateurs des systèmes, d'être en capacité de détecter dans les meilleurs délais tout incident ou cyber-attaque et de connaître les procédures pour y faire face.

Des mesures afférentes à la sécurité des systèmes d'information (SSI) doivent être mises en œuvre, notamment celles recommandées dans le cadre de la politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI MCAS) et de sa déclinaison sectorielle au travers de la politique générale de sécurité des systèmes d'information de santé (PGSSI-S) pour le secteur médico-social.

Les mesures relatives à la sécurité des systèmes d'information sont à intégrer dans la fiche de sécurité.

1.4. *La sensibilisation et la formation des professionnels et des usagers*

Une attention particulière sera portée à la sensibilisation de l'ensemble du personnel sur son rôle en matière de vigilance et de prévention au sein de son service et aux conduites à tenir en cas d'attentat sur site ou dans l'environnement immédiat de l'établissement.

Dans ce cadre, les directeurs présenteront à l'ensemble du personnel les dispositions actualisées du règlement de fonctionnement et, le cas échéant, leur fiche de sécurité et ils s'assureront que les consignes du plan Vigipirate et les mesures de protection propres à chaque site et à chaque service sont connues et maîtrisées.

Le personnel doit être préparé à réagir à une attaque terroriste. En lien avec les forces de sécurité intérieure, un plan de sensibilisation et de formation approprié leur sera dispensé. Il doit être en cohérence avec les modules de formation à la sécurité qui vont être mis en place lors de la formation initiale et continue à destination du personnel (*cf.* annexe 2).

Pour accompagner les ESSMS dans leurs actions de sensibilisation, des guides pédagogiques « réagir en cas d'attentat » à destination de l'ensemble des établissements ont été élaborés par les ministères chargés des affaires sociales et de la santé, en partenariat avec le secrétariat général de la défense et de la sécurité nationale (SGDSN). Ils peuvent être adaptés au secteur concerné et au mode d'accueil du public (lieu fermé ou ouvert, accueil de mineurs, etc.).

Il convient également d'inciter les établissements à sensibiliser les usagers et les prestataires aux problématiques de sécurité, notamment par un affichage spécifique (« attentif ensemble ») et par un paragraphe dédié dans le livret d'accueil ou la diffusion de vidéo ou de film.

2. **Le rôle des agences régionales de santé (ARS) et des directions régionales de la jeunesse, des sports et de la cohésion sociale (DR(D)JSCS) dans l'animation et la coordination de la politique régionale de sécurité dans le secteur social et médicosocial**

Les directeurs généraux des agences régionales de santé pour le secteur médico-social, et les directeurs régionaux de la jeunesse, des sports et de la cohésion sociale pour le secteur social, sont chargés en coordination avec les présidents de conseil départemental en cas de compétence conjointe, d'animer et de coordonner la politique régionale de sécurité qui couvrira notamment la prévention, la protection et la réaction face à des actes terroristes.

À cette fin, ils veilleront à :

– la définition explicitée par les ESSMS de leur stratégie de protection (l'actualisation du règlement de fonctionnement ou élaboration de la fiche de sécurité) ;
– l'accompagnement des établissements dans la démarche de sécurisation en les invitant notamment à participer à la conception et au suivi d'actions d'information et de sensibilisation en direction du personnel et des usagers ;
– l'application des mesures de prévention de la radicalisation, en lien avec le référent radicalisation de l'ARS ou de la DR(D)JSCS ;
– faciliter le retour d'expériences et le partage de pratiques entre ESSMS ;
– la cohérence des mesures de sécurité prises dans la région.

En outre, il est recommandé aux ARS d'associer des représentants des ESSMS devant élaborer une fiche de sécurité à leurs groupes d'appui techniques sur la sécurisation des établissements de santé.

Je vous prie de bien vouloir d'une part, vous assurer de la diffusion de cette instruction aux établissements et services sociaux et médico-sociaux relevant de votre champ de compétences et, d'autre part, de la transmettre aux présidents des conseils départementaux concernés pour information et éventuelle application aux ESSMS relevant de leur compétence.

Pour les ministres et par délégation :

Le secrétaire général des ministères chargés des affaires sociales, haut fonctionnaire de défense et de sécurité,
P. Ricordeau

Le directeur général de la cohésion sociale,
J.-P. Vinquant

ANNEXE 1

LIGNES DIRECTRICES POUR L'ÉLABORATION D'UNE FICHE DE SÉCURITÉ

PRÉAMBULE

Il revient à la direction de l'ESSMS de définir une politique globale de sécurité visant à protéger les personnes, les biens et les informations.

Cette politique doit :

– être appropriée à la nature et à l'étendue des menaces et vulnérabilités identifiées ;
– s'appuyer sur un responsable désigné, en charge de la sécurité de l'établissement ;
– définir les principaux objectifs d'amélioration continue en matière de sécurité ;
– être communiquée à tout le personnel afin de le sensibiliser sur son rôle en matière de sécurité ;
– être consignée par écrit, datée, testée et revue périodiquement, pour s'assurer qu'elle reste pertinente et appropriée.

DÉFINITION ET CONTENU

La fiche de sécurité traduit la politique et l'organisation de la sécurité de l'ESSMS :

– elle est fondée sur une analyse de risques de l'ensemble des espaces : périphériques, espace périmétrique, volumes intérieurs ;
– elle repose sur l'identification des vulnérabilités de la structure et fixe des priorités dans les sites à sécuriser ;
– elle précise les mesures organisationnelles à mettre en œuvre tant sur le plan de la vigilance, de la prévention que de la protection ;
– elle s'appuie sur l'expérience déjà acquise dans la gestion des problématiques liées à la sécurité et prend en compte la particularité de son environnement ;
– elle doit être élaborée en coordination avec les autorités (préfet, services municipaux et police ou gendarmerie) qui peuvent apporter leur expertise.

L'équipe de direction de la structure doit régulièrement passer en revue le système de gestion de la sécurité, pour s'assurer qu'il demeure pertinent, adéquat et efficace.

Il convient de distinguer :

– le dispositif de sécurité en temps normal ;
– le dispositif de sécurité en cas de crise locale ou en cas d'attentat.

En tout état de cause, la fiche de sécurité devra s'articuler avec les plans et règlementations existants (plan Vigipirate, plan communal de sauvegarde (PCS), plan bleu pour les établissements concernés, éventuel plan de continuité d'activité si l'établissement s'en est doté etc.).

DESCRIPTION DE L'ATTENDU

La fiche de sécurité s'articule autour de deux modes de fonctionnement.

1. **Sécurisation de l'ESSMS en temps normal**

La structure réalise un diagnostic initial qui lui permettra :

– d'identifier de façon régulière les risques et les menaces en lien avec les autorités locales (se tenir informé des mesures à mettre en œuvre dans le cadre du plan Vigipirate) ;
– d'évaluer ses vulnérabilités ;
– de mettre en œuvre des mesures adaptées pour supprimer ou réduire ces vulnérabilités, selon un calendrier et des priorités à définir en fonction des risques identifiés et de ses capacités.

Ces actions doivent être planifiées, y compris leur maintenance et leur surveillance, afin d'assurer qu'elles sont réalisées dans les conditions requises en :

- élaborant et en tenant à jour des procédures formalisées permettant la définition des conduites à tenir en situation normale comme en situation de crise concernant :
  - les exigences pertinentes aux fournisseurs, aux sous-traitants et partenaires et en vérifiant leur application ;
  - l'accueil des personnes extérieures (familles ou proches des résidents/usagers, intervenants extérieurs) ;
  - l'identification et de traitement des incidents et des actes de malveillance ;
- s'assurant que les procédures de gestion de crise sont connues de tous :
  - les procédures d'alerte interne et externe (nécessité d'afficher les numéros d'urgence internes ou externes prés de chaque poste téléphonique ou de les enregistrer dans les téléphones portables) ;
  - la fermeture en urgence de la structure ;
  - la mise à l'abri ;
  - les mesures de confinement ;
  - les procédures d'évacuation de l'établissement : horizontale (partielle) ou totale ;
- prenant contact avec les représentants locaux des forces de sécurité publique (commissariat ou brigade de gendarmerie de proximité) et de secours (le service départemental d'incendie et de secours (SDIS) et le SAMU) pour :
  - permettre une connaissance réciproque (il est souhaitable de pouvoir identifier un correspondant qui sera, au quotidien, l'interlocuteur privilégié du directeur pour les situations de violence et les problèmes de sécurité) ;
  - connaitre les éventuelles modalités de surveillance de la voie publique, notamment dans le cadre de Vigipirate ;
  - solliciter si besoin leur expertise en matière de sécurité ou leur présence lors d'exercices ;
  - transmettre au correspondant local de la police ou de la gendarmerie la fiche de sécurité et le plan à jour de l'établissement.

2. **Sécurisation complémentaire en situation d'attentat (ou de suspicion d'attentat) à proximité de l'établissement**

Il peut aborder notamment les quatre catégories d'informations suivantes.

2.1. *La fiche de sécurité doit indiquer comment déterminer s'il faut évacuer ou se confiner*

Dans tous les cas, si une consigne officielle a été communiquée par les forces de sécurité, elle doit être appliquée.

Dans l'attente de consigne officielle communiquée par les forces de sécurité :

- si l'attaque a lieu à l'extérieur du site, la mise à l'abri peut être préférée à l'évacuation ;
- si l'attaque a lieu à l'intérieur du site, les mesures d'évacuation ou de mise à l'abri doivent être envisagées en fonction des circonstances et des lieux ;
- pour envisager une évacuation, il faut réunir 3 conditions : avoir identifié la localisation exacte du danger ; la majorité des personnes présentes sur le site peuvent s'échapper sans risque ; l'alerte a bien été donnée en interne et en externe.

2.2. *La fiche de sécurité doit indiquer comment donner l'alerte à l'ensemble du personnel*

En cas d'attentat au sein de la structure, l'urgence est, dès que possible, de donner l'alerte : en interne pour que les personnes évitent de s'exposer au danger et s'adaptent à la situation, et en externe pour que les forces de l'ordre puissent intervenir pour neutraliser les assaillants et prévenir un éventuel sur-attentat.

- La fiche de sécurité doit exposer la méthode retenue pour transmettre l'alerte en cas de situation d'urgence de type attentat. Si des méthodes différentes ont été retenues selon que la situation d'urgence survient dans l'établissement ou à proximité de l'établissement, la fiche de sécurité doit le préciser.

2.3. *La fiche de sécurité doit prévoir comment se confiner*

À ce titre, la fiche doit indiquer :

– sur un plan à jour des locaux, la ou les salle(s) présélectionnées pour se mettre à l'abri ; le choix de plusieurs salles est à privilégier dans le cas d'une structure disposée sur différents étages ;

– la possibilité d'une communication discrète entre les personnes présentes dans chaque salle de mise à l'abri doit avoir été envisagée ;

– pour chaque salle de mise à l'abri, le comportement (éteindre les lumières…), le mobilier (tables, armoires…) ou les aménagements (volets roulants…) utiles pour se barricader et se protéger ;

– pour chaque salle de mise à l'abri, la liste des équipements et activités nécessaires afin de prendre soin des résidents.

2.4. *La fiche de sécurité doit prévoir comment évacuer*

À ce titre, la fiche de sécurité doit indiquer :

– sur un plan à jour des locaux, le parcours privilégié d'évacuation, qui doit prendre en compte l'âge et la mobilité, ainsi que l'encombrement éventuel des moyens de transport notamment lorsque les pièces de vie sont situées en étage ;

– que ce parcours privilégié est susceptible d'être changé en considération de la localisation exacte du danger dans l'hypothèse où la situation d'urgence surviendrait dans l'établissement ;

– sur un plan à jour des abords de l'établissement, les lieux vers lesquels évacuer et se mettre en sécurité, prédéfinis en accord avec leurs responsables (commissariat, mairie, voisinage…). Plusieurs lieux de repli peuvent être prédéfinis, afin d'être en mesure de savoir où aller quelles que soient les directions d'où venait le danger et dans laquelle la fuite a eu lieu.

3. **Les mesures spécifiques à la sécurité des systèmes d'informations**

Les systèmes d'information, devenus essentiels aux différentes actions quotidiennes des établissements, à la qualité des soins et à la prise en charge des usagers et des patients, se trouvent confrontés à des sources de menaces qui croissent en nature et en nombre et au développement de la cybercriminalité.

La cybercriminalité se définit communément comme toute action illicite visant l'intégrité d'un site informatique déterminé, ou bien menée à l'aide d'un outil informatique. La transformation numérique rapide du secteur social et médico social nécessite de tenir compte de ces nouveaux risques.

De nombreux exemples ont récemment mis en lumière ces menaces contre les secteurs de la santé et du social. Les cyberattaques menées contre de systèmes d'information insuffisamment protégés entraînent des conséquences financières, de temps passé et de gêne professionnelle très élevées :

– certains virus permettent de détruire très rapidement des volumes considérables de données ou mettent hors-service un ordinateur. Ces situations conduisent parfois à devoir réinstaller tout le parc informatique et à reconstituer les données, et ce avec un coût élevé pour un résultat souvent très partiel ;

– des altérations (effacement par erreur, modifications indues…) de données, parfois essentielles, se produisent régulièrement ;

– des systèmes d'information se retrouvent accessibles depuis Internet, par de simples requêtes à travers des moteurs de recherche tels que Google, Yahoo, Bing… Ils sont souvent disponibles sur Internet soit par erreur, soit après avoir été confiés à des fournisseurs de services dont la sécurité est défaillante. Ces incidents se traduisent par une médiatisation dommageable pour l'ensemble du secteur social et médico-social ; sans préjudice d'éventuelles poursuites pénales engagées par les usagers qui en sont victimes ; l'installation de logiciels informatiques malveillants, prennent en otage les données. Le ransomware, ou rançongiciel, chiffre et bloque les fichiers contenus sur l'ordinateur et une rançon est demandée en échange d'une clé permettant de les déchiffrer.

Dans un contexte marqué par la recrudescence des malveillances informatiques et des surfaces d'attaque pesant sur des systèmes d'information insuffisamment protégés, l'application des principes suivants s'avère essentielle :

– s'assurer que les logiciels sont régulièrement mis à jour ;
– s'assurer que tous les ordinateurs connectés à Internet sont équipés d'un logiciel antivirus et protégés par un pare-feu ;
– réduire les risques d'attaques informatiques en ne connectant sur le réseau que des matériels informatiques à usage professionnel ;
– sauvegarder les informations (sauvegarde au minimum hebdomadaire, avec une conservation des sauvegardes mensuelles sur 12 mois glissants et annuelles), en conservant de préférence une copie sécurisée dans un lieu différent ;
– verrouiller la session de travail en quittant le poste ou de façon automatique au bout d'un temps d'inactivité, généralement de l'ordre de 30 minutes mais à adapter à l'organisation du travail ;
– s'assurer que l'accès aux ordinateurs est protégé par des mots de passe individuels contrôlés de manière sécurisée, utiliser des mots de passe non triviaux, de 10 caractères (mêlant chiffres, lettres et caractères spéciaux) et changés régulièrement ;
– élaborer un mode de fonctionnement dégradé dans le cadre du plan de continuité d'activité si l'établissement s'en est doté, qu'il convient de tester régulièrement ;
– sensibiliser l'ensemble du personnel et des intervenants aux bonnes pratiques d'utilisation des systèmes d'information. Des actions de sensibilisation, et de formation doivent être organisées régulièrement ;
– mettre en œuvre à l'intention du personnel une politique d'utilisation acceptable concernant la navigation sur Internet, la messagerie électronique, les salons de discussion, les sites de réseaux sociaux, les sites marchands et les sites de téléchargement de jeux et de musique.

Un ensemble de guides et référentiels sont indiqués dans les documents de référence.

4. **Organisation d'exercices**

Des exercices réguliers sont recommandés afin de tester le dispositif de sécurité, si possible en lien avec les services de sécurité concernés, et son appropriation par le personnel.

La réalisation d'exercices peut prendre plusieurs formes :

– rappel simple des procédures et du rôle de chacun par le responsable du site ou son chargé de sûreté ;
– exercice «sur table» au cours duquel, dans une salle, les employés présentent la réaction qu'ils auraient en cas d'attaque. Celle-ci doit être scénarisée (lieu, nombre et armes des assaillants identifiés) ;
– test technique du système d'alerte ;
– organisation de reconnaissances exploratoires (lieux d'évacuation, salles de confinement, etc.) ;
– exercice de mise en situation avec des personnes simulant l'intrusion (les employés doivent être prévenus de la réalisation de l'exercice mais pas nécessairement de sa date exacte pour éviter des phénomènes de panique). La police ou la gendarmerie sont invités à apporter leur expertise. Ce type d'exercice doit être planifié et préparé en lien étroit avec les préfectures et les responsables des services locaux de sécurité concernés.

5. **Mise à jour de la fiche de sécurité**

La fiche de sécurité fait l'objet de mises à jour périodiques, notamment à la suite des enseignements tirés des exercices.

Ces retours d'expérience doivent pouvoir être partagés au niveau régional et local, en lien avec l'ARS et son groupe d'appui, les services de cohésion sociale, ou les services du conseil départemental.

DOCUMENTS DE RÉFÉRENCE

Sécurisation des établissements

Vigipirate

- Plan Vigipirate du 1er décembre 2016 « Faire face ensemble »[1]
- Guides « Vigilance attentats : les bons réflexes » à destination des équipes de direction et du personnel des établissements de santé, sociaux et médico-sociaux (juin 2016)[2]
- Guide « Gérer la sûreté et la sécurité des événements et sites culturels » (avril 2017)[3]

Ministères sociaux

- Guide de déclinaison des mesures de sécurisation périmétrique et bâtimentaire
- Guide d'aide à l'élaboration d'un plan de sécurisation d'établissement (PSE) relatif aux établissements de santé[4]
- Guide méthodologique ONVS – La prévention des atteintes aux personnes et aux biens en milieu de santé (avril 2017[5]
- Points clefs d'une politique de sécurité (document DGOS/FHF)[6]
- Guide «sûreté dans les établissements d'accueil du jeune enfant », se préparer et faire face aux situations d'urgence particulière (avril 2017)[7]

Sécurité des systèmes d'information

Ministères sociaux

- Politique de sécurité des systèmes d'information pour les ministères chargés des affaires sociales (PSSI MCAS). Arrêté du 1er octobre 2015 portant approbation de la PSSI MCAS. NOR : AFSZ1523362A[8]
- Politique générale de sécurité des systèmes d'information de santé (PGSSI-S) : référentiels et guides pratiques qui traitent de la sécurisation de données de santé[9]
- Instruction no SG/DSSIS/2016/309 du 14 octobre 2016 relative à la mise en œuvre du plan d'action SSI. NOR : AFSZ1629742J[10]

Agence nationale de la sécurité des systèmes d'information (ANSSI)

- Guide d'hygiène informatique : édicte des règles élémentaires et applicables pour tout système d'information. La fiche sécurité inclura les mesures prévues afin de répondre à chacune des mesures[11]
- Guides des bonnes pratiques[12]

[1] http://www.gouvernement.fr/risques/le-citoyen-au-coeur-du-nouveau-dispositif-vigipirate

[2] http://www.sgdsn.gouv.fr/vigipirate/guide-a-destination-des-equipes-de-direction-des-etablissements-de-sante-sociaux-et-medico-sociaux/

[3] http://www.culturecommunication.gouv.fr/Presse/Communiques-de-presse/Gerer-la-surete-et-la-securite-des-evenements-et-sites-culturels

[4] http://solidarites-sante.gouv.fr/IMG/pdf/guide_d_aide_a_l_elaboration_du_pse_-_version_avril_2017.pdf

[5] http://solidarites-sante.gouv.fr/IMG/pdf/guide_onvs_-_prevention_atteintes_aux_personnes_et_aux_biens_2017-04-27.pdf

[6] http://solidarites-sante.gouv.fr/IMG/pdf/Fiches_reflexes_ONVS.pdf

[7] http://www.egalite-femmes-hommes.gouv.fr/wp-content/uploads/2017/04/FINAL_mise-a-jour_24-avril_guide-Securite_EAJE.pdf

[8] https://www.legifrance.gouv.fr/eli/arrete/2015/10/1/AFSZ1523362A/jo/texte

[9] http://esante.gouv.fr/

[10] http://circulaire.legifrance.gouv.fr/index.php?action=afficherCirculaire&hit=1&r=41533

[11] https://www.ssi.gouv.fr/uploads/2017/01/guide_hygiene_informatique_anssi.pdf

[12] https://www.ssi.gouv.fr/administration/bonnes-pratiques/

ANNEXE 2

SENSIBILISATION ET FORMATION DES PROFESSIONNELS

Une attention particulière sera portée à la sensibilisation et à la formation de l'ensemble du personnel sur son rôle en matière de vigilance, de prévention et de réaction dans le cadre de l'amélioration de la sécurité de la structure. Il s'agit de développer une véritable « culture de la sécurité », propre à permettre une réaction collective face à des risques et à des menaces.

Le volet information :

- informer le personnel sur les risques et les menaces et sur le plan Vigipirate ;
- développer une stratégie de sensibilisation interne *via* l'affichage (*cf.* posture Vigipirate) et en diffusant des messages de vigilance sur le réseau interne et la vidéo « réagir en cas d'attaque terroriste » ;
- présenter la fiche de sécurité au personnel en expliquant ses finalités et les zones et secteurs considérés comme les plus sensibles ;
- sensibiliser le personnel au respect des mesures de sécurité et de vigilance:
  - rappel des procédures et du rôle de chacun ;
  - information sur la procédure de signalement et l'identification des « signaux faibles » (incidents mineurs, comportements suspects, etc.) qui peuvent précéder un attentat ;
- diffuser les guides de bonnes pratiques en matière de vigilance.

Le volet formation :

Avec l'appui des écoles de formation professionnelles, dont l'École des hautes études en santé publique (EHESP) et les écoles de formation d'infirmiers, des modules de formation initiale et continue à destination des chefs d'établissement, du personnel médical et paramédical seront mis en place à partir de 2017.

En complément, des formations ciblées seront organisées par la structure visant à :

- la formation aux premiers secours (pour mémoire, les responsables d'établissement mettent en œuvre les dispositions prévues aux articles R. 4224-15 et R. 4224-16 du code du travail) ;
- la connaissance et la maîtrise, par tous des moyens d'alerte (diffusion de l'alerte et connaissance des signaux d'alerte) ;
- la connaissance du site, en organisant des «reconnaissances exploratoires» afin d'identifier les cheminements, les issues de secours, les obstacles éventuels, et tout ce qui peut offrir une protection ;
- des mises en situation simples et des exercices collectifs, intégrant les différents partenaires, et en exploitant systématiquement les retours d'expérience de ces exercices.

Sur demande, les services de formation nationaux et locaux et les services spécialisés du ministère de l'intérieur pourront apporter leur concours à l'organisation de séances de sensibilisation et aux modules de formation développés par l'établissement.

Il est conseillé de s'appuyer sur les formations dispensées en local par les préfectures et les forces de sécurité intérieure aux acteurs de l'ensemble des secteurs sociaux-économiques.

Documents de référence

Plan Vigipirate du 1er décembre 2016 « Faire face ensemble ».[1]

Guides « Vigilance attentats : les bons réflexes » à destination des équipes de direction et du personnel des établissements de santé, sociaux et médico-sociaux (juin 2016).[2]

Code du travail : Art R. 4224-15 et R. 4224-16.

[1] http://www.gouvernement.fr/risques/le-citoyen-au-coeur-du-nouveau-dispositif-vigipirate

[2] http://www.sgdsn.gouv.fr/vigipirate/guide-a-destination-des-equipes-de-direction-des-etablissements-de-sante-sociaux-et-medico-sociaux/