Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail[1]	Actions à prendre / état de la situation
Norme 4.1 Chaque institution de sécurité sociale connectée au réseau de la Banque Carrefour doit disposer d'une politique formelle de sécurité de l'information qui est actualisée en permanence.	Politique de sécurité	Conseiller en sécurité	-	1 jour	**Plan d'action** Récupérer la politique formelle de sécurité mise à disposition par la BCSS et l'adapter aux besoins internes du CPAS. Proposer et faire valider la politique de sécurité adaptée par Conseil de l'aide sociale / le bureau permanent. **Planning.** Présentation au Bureau Permanent au cours du premier trimestre et suivi au cours des autres trimestres.
Norme 4.2 **4.2. Organisation de la sécurité**	Organisation				
4.2.1. Chaque institution de sécurité sociale connectée au réseau de la Banque Carrefour doit:					
4.2.1.1. organiser, en son sein, un service de sécurité de l'information placé sous la direction d'un conseiller en sécurité de l'information ou confier la tâche à un service spécialisé de sécurité de l'information.		Secrétaire / Président / Bureau permanent	1 j/sem	1 j/sem	**Plan d'action.** Faire nommer un conseiller en sécurité par le bureau permanent**.** Présentation au Bureau Permanent au cours du premier trimestre et suivi au cours des autres trimestres.
4.2.1.2. communiquer l'identité de son conseiller en sécurité et de ses adjoints éventuels au service de sécurité du SPP IS.		Conseiller en sécurité	-	1 heure	Envoyer la décision officielle du Conseil de l'aide sociale / Bureau Permanent au SPP IS.
4.2.1.3. disposer d'un plan de sécurité approuvé par l'instance responsable de l'institution concernée.		Conseiller en sécurité	1 jour	1 jour	Sur base de l'inventaire des faiblesses constatées par rapport aux normes minimales, dresser un plan d'action destiné à corriger ces faiblesses en 3 ans ou plus.

[1] La charge de travail dépend beaucoup de la taille du CPAS.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.2.1.4. disposer des crédits de fonctionnement nécessaires approuvés par l'instance responsable de l'institution concernée et inscrits dans un budget de sécurité défini séparément, afin de pouvoir prévoir l'exécution de son plan de sécurité.		Bureau permanent		30'	Faire avaliser par le bureau permanent les dépenses prévues dans le plan de sécurité. Avec l'aval du/de la secrétaire, demander au responsable des finances d'inscrire les dépenses relatives à la sécurité informatique dans un poste budgétaire distinct.
4.2.1.5. communiquer au SPP IS le nombre d'heures que le CPAS a officiellement attribuées à son conseiller en sécurité et à ses adjoints éventuels pour l'exécution de leurs tâches (4).		Conseiller en sécurité	-	1 heure	Envoyer au SPP IS le document officiel du Bureau permanent précisant le nombre d'heures officiellement attribuées au conseiller. **Attention** : *le nombre d'heures dépend de l'ensemble des activités à réaliser pendant l'année.* *Exemples d'activités :* - *régularisation des licences antivirus : 2 heures/an ;* - *suivi des incidents physiques (alarmes, vols, pannes, dégâts, virus, loggings des utilisateurs, loggings des utilisateurs de l'application sociale, …….) : x heures ;* - *réponse au questionnaire de la BCSS : 4h/an ;* - *contacts avec les fournisseurs des logiciels, examen des faiblesses, examen des incidents informatiques, formation, sensibilisation du personnel à la sécurité, élaboration d'une charte de bonne utilisation d'internet, du mail, création d'une procédure de sauvegarde des fichiers et des données, etc.*

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.2.1.6. les conseillers en sécurité concernés veillent, au sein de leur propre institution, à l'utilisation sécurisée de la carte professionnelle pour soins de santé comme prévu aux articles 42 à 50 de l'arrêté royal du 22 février 1998		Conseiller en sécurité		1 heure	Etablir un inventaire de tous les de lecteurs de cartes Sam (les cartes SAM sont des cartes permettant de lire les cartes SIS) et de tous les utilisateurs. Mettre à jour les inventaires de cartes SAM et des utilisateurs chaque fois que la situation change.
4.2.1.7. disposer de procédures en vue de la communication d'informations au conseiller en sécurité de sorte que ce dernier possède les données lui permettant d'exécuter la mission de sécurité lui confiée.		Secrétaire et conseiller en sécurité et toute autre personne concernée	-	A mesurer	Organiser le recueil d'informations via une réunion périodique de sécurité avec les chefs de service concernés. Elaborer une procédure avec le service du personnel pour prévoir l'arrivée des nouveaux engagés et les départs afin de régler les problèmes d'accès au réseau. Créer un système d'allocations d'accès, de suppression et de récupération d'accès selon une procédure écrite ou informatisée laissant des traces. Créer des procédures simples visant à impliquer les autres services et à récolter toutes les informations impactant la sécurité (panne de serveur, panne d'air conditionné, système de contrôle d'accès en panne, incidents…). Eventuellement, créer un registre des incidents accessibles à tous.
4.2.1.8. disposer de procédures ayant pour objectif d'organiser la concertation avec les différentes parties impliquées[2] afin d'associer plus étroitement les conseillers en sécurité aux travaux de l'institution.			A mesurer	A déterminer	Idem.

[2] Les parties visées par cette norme sont principalement les membres du service informatique, le conseiller en prévention, le conseiller en sécurité et les services qui gèrent les données.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.3. Sécurisation physique et sécurisation de l'environnement	Sécurité physique				
Chaque institution de sécurité sociale connectée au réseau de la Banque Carrefour doit:					
4.3.1. limiter aux personnes autorisées et contrôler, aussi bien pendant qu'en dehors des heures de service, les accès aux bâtiments et aux locaux.		Conseiller en sécurité, secrétaire et responsable SIPP.	A mesurer	A déterminer	Sécuriser les accès physiques au CPAS en fonction des risques créés par l'environnement. Veiller à ce que personne ne puisse rentrer dans le CPAS sans devoir s'annoncer. Si la disposition des lieux le permet, il n'est pas nécessaire d'installer un système de contrôle d'entrée automatisé. Veiller à ce que personne ne puisse se promener dans le CPAS sans être accompagné.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.3.2. prendre des mesures pour la prévention, la protection, la détection, l'extinction et l'intervention concernant l'incendie, l'intrusion et les dégâts des eaux.		Conseiller en sécurité, secrétaire et responsable SIPP.	A estimer en fonction des besoins	1 jour par mois ou plus selon les besoins	Organiser une ou plusieurs équipes d'évacuation et faire une simulation chaque année. Prévenir la première année du jour de la simulation, prévenir la deuxième année de la semaine au cours de laquelle la simulation aura lieu. Faire un bilan de l'évacuation après la simulation et corriger les faiblesses sur une liste des actions à mener pendant l'évacuation (fermeture des portes, vérification que plus personne n'est resté, etc.).. Organiser une équipe d'intervention si nécessaire et prévoir une formation de base de qualité soit auprès des pompiers de la commune soit auprès d'un organisme ou une société spécialisé. Faire un inventaire des risques liés à l'incendie, aux dégâts des eaux et au gaz. Vérifier l'état de sécurisation des locaux (alarme intrusion, verrouillages à codes, etc.), veiller à occulter les locaux contenant du matériel de valeur (teinture, stores), faire l'inventaire des mesures existantes ou à installer (extincteur à installer, porte s'ouvrant avec une barre anti-panique, …). Impliquer le responsable SIPP, les pompiers, la police ou la société spcialisée pour diminuer les risques. Examiner chaque fois diverses solutions, évaluer la nécessité d'investir dans la protection automatique ou non. Apporter une attention particulière à l'air conditionné et aux contrats de maintenance.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.3.2. prendre des mesures pour la prévention, la protection, la détection, l'extinction et l'intervention concernant l'incendie, l'intrusion et les dégâts des eaux (suite).					Contrôler l'existence et la nécessité de disposer d'un contrat d'assistance et de remplacement de matériel informatique en cas de panne ou de sinistre technique.Vérifier également la couverture des assurances.
4.3.3. lorsqu'elle fournit des données dans le cadre de la sécurité sociale disposer d'une alimentation électrique alternative permettant de clôturer sans risque les opérations informatiques.		Conseiller en sécurité et responsable informatique	1/2 jour	1/2 jour	Cette alimentation électrique peut être : - pour les gros CPAS, un moteur diesel, un système de batterie, une alimentation alternative, un UPS limité à une batterie, etc. - pour les CPAS ayant une petite informatique, un UPS avec batterie dont le programme est installé sur le serveur et permettant de terminer les opérations en cours sans perdre de données. Il est important de vérifier que les batteries sont toujours en ordre de fonctionnement (ainsi que les autres systèmes) et d'organiser un test de fonctionnement à partir d'une simulation.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.4. Sécurisation logique de l'accès	Sécurité informatique				
4.4.1. sécuriser l'accès aux données[3] nécessaires à l'application et à l'exécution de la sécurité sociale par un système d'identification, d'authentification et d'autorisation.		Conseiller en sécurité et responsable informatique	A estimer sur base des besoins	Idem	Créer un nom d'utilisateur pour chaque utilisateur et lui imposer un mot de passe à 8 caractères ou symboles à changer tous les trois mois. L'utilisateur doit pouvoir choisir seul son mot de passe qui ne doit pas être connu du conseiller en sécurité ni de l'informaticien. En cas de nécessité, mettre le mot de passe sous enveloppe scellée et signée à disposition du gestionnaire de réseau et de son adjoint ou de la personne désignée en cas d'absence.
4.4.2. implémenter un système de logging pour les données à caractère personnel nécessaires à l'application et à l'exécution de la sécurité sociale.		Conseiller en sécurité informatique, responsable informatique, fournisseur application sociale	A estimer	Idem	Les systèmes de loggings doivent permettre de savoir qui a fait quoi et quand surtout: 1. au niveau des connexions au réseau de la sécurité sociale par les utilisateurs ; 2. dans les applications utilisées par les assistants sociaux et les administratifs ; 3. dans toute application impliquant des échanges de données avec l'extranet de la sécurité sociale (réseau BCSS) et toute application de nature sensible contenant des données à caractère social. Ces loggings impliquent également leur conservation : mode de conservation (sur quel support), durée, protection, but, etc.

[3] Dans la présente norme, on entend par le terme "donnée" non seulement les données sociales à caractère personnel mais aussi tous les éléments logiques du système d'information qui assurent le traitement; par exemple les programmes, les applications, les fichiers, les utilitaires de système et autres éléments du système d'exploitation.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.4.3. mettre en place un système de copie de sécurité (back-up), régulièrement contrôlé, permettant de s'assurer, en cas de sinistre total ou partiel, qu'aucune perte de données irréparable ne puisse survenir (données nécessaires à l'application et à l'exécution de la sécurité sociale ainsi que celles concernant les applications et le système d'exploitation)		Conseiller en sécurité informatique, responsable informatique, fournisseur application sociale	2 jours	Idem	La mise en place de systèmes de back-ups doit répondre à plusieurs impératifs : - assurer la sauvegarde des données utilisées et ce pour la durée nécessaire au bon redémarrage des activités du CPAS, exemple : la durée de conservation des back-ups doit permettre au CPAS de pouvoir effectuer les paiements (éventuellement sur base des derniers paiements effectués) ; - assurer la sauvegarde des systèmes d'exploitation pour pouvoir tout réinstaller en cas de sinistre ; - disposer d'un système de vérification de la bonne sauvegarde des back-ups afin de pouvoir remplacer les supports informatiques à temps ; - assurer leur sauvegarde en un lieu extérieur au CPAS.
4.4.4. installer un système et des procédures formelles et actualisées permettant de détecter des infractions à la sécurité, de les suivre et de les réparer.		Conseiller en sécurité informatique, responsable informatique, fournisseur de l'application sociale.	Un IDS coûte minimum 2.000 € sans le personnel adéquat.	Un IDS impose la présence d'une personne chaque jour à temps plein derrière l'écran de contrôle.	A moins d'installer un IDS utilisable seulement par des CPAS ayant de gros moyens, seule une procédure purement administrative reposant sur la communication officielle d'anomalies constatées par des utilisateurs répond à cette norme. La constatation d'anomalies peut également être réalisée par le conseiller en sécurité en vérifiant les logs des systèmes d'audit disponibles à partir d'XP pro ou de tout autre environnement disposant de systèmes d'audit et de sécurité intégrée.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.4.5. Lorsque dans la zone « USERID » de la partie préfixe d'un message qu'elle adresse à la Banque Carrefour, l'institution reprend le numéro du programme qui a généré le message qu'elle adresse à la Banque carrefour bien qu'une personne physique soit à l'origine du message, la Banque Carrefour peut, à posteriori, retrouver le numéro de ce programme. La Banque Carrefour ne connaît cependant pas l'identité de la personne physique qui a émis ce message. Dans ce cas, c'est donc à l'institution sociale qu'il revient de faire la relation entre le numéro de programme qu'elle reprend dans la partie préfixe du message, qu'elle adresse à la Banque Carrefour, et l'identité de la personne physique qui émet le message.		Conseiller en sécurité informatique, responsable informatique, fournisseur application sociale	½ jour	½ jour	Procédure et inventaire des utilisateurs à réaliser avec la firme informatique fournisseur de l'application sociale si le CPAS fait appel à leurs services et avec l'informaticien responsable. Exemple. Il y a lieu d'établir une procédure liée à l'octroi, à la suppression des noms ou numéros des utilisateurs, et à l'inventaire des identités des utilisateurs puisque leurs accès doivent y être précisés. Cet inventaire doit être constamment à jour. Rien n'empêche le CPAS de demander à son fournisseur de logiciel de respecter cette norme.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.5. Développement, production et maintenance des applications Chaque institution de sécurité sociale connectée au réseau de la Banque Carrefour doit:					
4.5.1. disposer de procédures formelles et actualisées pour la mise en production de nouvelles applications et la réalisation d'adaptations aux applications existantes afin d'éviter qu'une seule et même personne n'assure le contrôle de ce processus.		Conseiller en sécurité informatique, responsable informatique, fournisseur application sociale	A évaluer	A évaluer	Cette norme est applicable uniquement par les CPAS développant eux-mêmes leurs applications. Cela n'empêche nullement un CPAS de demander à ses fournisseurs de logiciels de respecter cette règle.
4.5.2. disposer de procédures formelles et actualisées en vue d'élaborer la documentation lors du développement de nouvelles applications et systèmes et lors de la maintenance des applications et systèmes existant[4].		Conseiller en sécurité informatique, responsable informatique, fournisseur application sociale	5 jours	5 jours	La tenue à jour de la documentation est importante. Pour les CPAS travaillant avec des fournisseurs d'applications de quelque nature qu'elles soient, il est important qu'ils prévoient dans leur contrat la sauvegarde de leurs applications (codes sources) auprès d'un tiers de confiance (notaire, huissier, autorité, etc.) ainsi que la documentation en cas de faillite du fournisseur. Il est prudent de prévoir à intervalle régulier la remise à jour de la version et de la documentation auprès du tiers de confiance. *Exemples :* - *faire déposer auprès d'un notaire un exemplaire des codes source du programme*

[4] Dans la présente norme, on entend par "système" les éléments logiques qui font partie d'un système d'information. Bien que les fichiers, applications, etc (voir la note de bas de page n°7), tombent sous cette définition, il s'agit dans ce contexte plutôt de composantes au "niveau du système". Appliqués à un environnement mainframe de IBM, les exemples suivants peuvent être cités à titre de précision: CICS, DB2, RACF, VTAM, OPC, TSO, SMS, JES2, fichiers contenant des paramètres système, une présentation schématique de la construction logique du système d'information.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
					- *et veiller chaque année à ce que la dernière version actualisée ait été déposée,* - *exiger des garanties pour éviter les problèmes de reprise d'application par une autre société, en cas de faillite, en cas de non renouvellement de licence extérieure,…*
4.6 Protection du réseau. 4.6.1 Chaque CPAS connecté au réseau de la Banque carrefour doit :					
4.6.1.1 limiter l'accès au(x) système(s) informatique(s) aux personnes/objets identifiés, authentifiés et autorisés.	Sécurité physique et informatique.	Conseiller en sécurité, responsable informatique / service spécialisé dans la sécurité de l'information	Selon les coûts de sécurité à réaliser.	Selon le nombre d'utilisateurs et l'environnement utilisé.	Mettre dans des locaux prévus à cet effet tous les systèmes permettant la gestion du réseau informatique, limiter les accès aux systèmes informatiques (serveurs, modems, routeurs, switches, etc.) aux seules personnes concernées (le gestionnaire système, le responsable réseau, le fournisseur). *Exemples :* - *installer un clavier numérique pour limiter aux possesseurs du code l'accès au centre de calcul,* - *installer un système de contrôle d'entrée à badge,* - *limiter l'accès au centre de calcul en ne donnant qu'une clef aux deux personnes admises mais en confiant un troisième exemplaire sous enveloppe scellée au responsable du CPAS ou à une personne désignée (secrétaire, Président, conseiller, etc.).*

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.6.1.2. installer un système et des procédures formelles et actualisées permettant la détection, le suivi et la réparation d'infractions au niveau de la sécurité.	Sécurité informatique	Conseiller en sécurité informatique, responsable informatique, fournisseur application sociale	Un IDS coûte minimum 2.000 € sans le personnel adéquat.		A moins d'installer un IDS[5] utilisable seulement par des possesseurs de gros systèmes, seule une procédure purement administrative reposant sur la communication officielle d'anomalies constatées par des utilisateurs répond à cette norme. La constatation d'anomalies peut également être réalisée par le conseiller en sécurité en vérifiant les logs des systèmes d'audit disponibles à partir du Windows 2000 ou de tout autre environnement disposant de systèmes d'audit et de sécurité intégrée tel le moniteur réseau
4.6.3. Les CPAS peuvent utiliser l'Extranet de la sécurité sociale pour les liaisons TCP/IP externes à la sécurité sociale. Pour leurs liaisons directes avec les réseaux TCP/IP externes à la sécurité sociale, les CPAS doivent mettre en œuvre des mesures de sécurité qui restent conformes aux mesures prises au niveau de l'Extranet de la sécurité sociale	Sécurité informatique	Conseiller en sécurité, responsable informatique			Il est bon de savoir qu'un réseau interne parfaitement sécurisé n'est efficace que si l'on contrôle toutes ses entrées. Dès lors, il faut s'assurer que toutes les connexions vers l'extérieur obéissent aux mêmes règles de sécurité, c'est à dire au moins aux normes minimales.
4.7. Plan de continuité. Chaque CPAS connecté au réseau de la Banque carrefour doit :					

[5] Intrusion detection system : il s'agit d'un programme informatique permettant de détecter des tentatives d'intrusion et de piratage.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.7.1. réaliser une analyse de risques permettant l'élaboration d'un plan de continuité.	Organisationnelle	Conseiller en sécurité		Selon l'importance du CPAS et de la quantité de risques, plusieurs heures à plusieurs jours.	Reprendre chaque aspect de la sécurité exposé dans la partie consacrée aux conditions minimales de sécurité et estimer quels sont les problèmes qui pourraient se poser en pratique au CPAS en cas de catastrophe. Il faut alors évaluer la probabilité de survenance de l'incident et l'impact sur la gestion de l'établissement : un risque élevé mérite une attention toute particulière.
4.7.2. élaborer, tester et maintenir un plan de continuité afin de pouvoir garantir les missions de sécurité sociale du CPAS. En outre, il doit prévoir un centre de migration informatique en cas de sinistre partiel ou total.	Organisationnelle	Conseiller en sécurité, responsable informatique et toute personne concernée			En fonction des points qui ont été relevés dans l'analyse de risques, le conseiller en sécurité décrit dans le plan de continuité toutes les étapes à entreprendre en cas d'incident. Il est important que chaque personne qui est amenée à intervenir soit au courant des dispositions du plan de continuité, afin que même en l'absence du conseiller en sécurité, des mesures puissent être prises pour faire redémarrer le CPAS dans les délais qu'il s'était déterminé.
4.8. Inventaire Chaque CPAS connecté au réseau de la Banque carrefour doit :					
4.8.1 disposer d'un inventaire du matériel informatique et des logiciels qui est mis à jour en permanence	Sécurité physique	Conseiller en sécurité	Selon le nombre d'utilisa-teurs.	Une à plusieurs heures (parfois des jours pour les gros CPAS).	Cet inventaire vise à établir une liste complète des programmes, matériels, réseaux … utilisés afin de permettre, en cas de désastre majeur, de reconstruire, en fonction de priorités, un environnement de travail le plus complet et le plus adéquat possible. Procédure et inventaire à réaliser avec la firme informatique fournisseur de l'application sociale si le CPAS fait appel à leurs services et avec l'informaticien responsable.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
					Exemple : il existe des petits programmes utilitaires auprès des fournisseurs qui permettent de faire automatiquement l'inventaire des programmes Il y a lieu d'établir une procédure liée à l'octroi, à la suppression des noms ou numéros des utilisateurs, des mots de passe et à l'inventaire des identités des utilisateurs puisque leurs accès doivent y être précisés. Cet inventaire doit être constamment à jour. *Exemple :* *Embauche – service du personnel – information auprès du responsable du service, du service informatique et du conseiller en sécurité – demande d'accès par le responsable de service auprès soit de l'informatique, soit du conseiller en sécurité.* *L'ensemble de ces formalités suppose une trace écrite : note standard ou mail*
4.9. Protection contre les infections par les virus informatiques. Chaque CPAS connecté au réseau de la Banque Carrefour doit:					
4.9.1. disposer d'un manuel d'utilisation relatif à la prévention d'infection par les virus, au fonctionnement du logiciel anti-virus installé et aux actions à entreprendre en cas d'infection par un virus.	Sécurité informatique	Responsable informatique et le service informatique	Néant	Néant	Le manuel est livré avec le logiciel. Il est prudent de le lire et de procéder aux opérations nécessaires (disquette de redémarrage) pour pouvoir agir en cas de présence de virus sur un PC ou sur le réseau.

Norme minimale	Type de sécurité	Responsable	Coût estimé	Charge de travail	Actions à prendre / état de la situation
4.9.1. disposer d'un manuel d'utilisation relatif à la prévention d'infection par les virus, au fonctionnement du logiciel anti-virus installé et aux actions à entreprendre en cas d'infection par un virus.	Sécurité informatique	Responsable informatique et le service informatique	Néant	Néant	Le manuel est livré avec le logiciel. Il est prudent de le lire et de procéder aux opérations nécessaires (disquette de redémarrage) pour pouvoir agir en cas de présence de virus sur un PC ou sur le réseau.
4.9.2. installer un logiciel anti-virus actualisé afin de prévenir, de détecter et de corriger des infections par des virus informatiques.	Sécurité informatique	Responsable informatique et le service informatique	Selon le nombre d'utilisa-teurs.	Une à plusieurs heures (parfois des jours pour les gros CPAS).	La simple installation du programme antivirus n'est pas une solution en tant que telle, il faut encore tenir à jour ce programme notamment en lui indiquant les nouveaux virus découverts afin qu'il puisse les détecter. C'est ce qu'on appelle tenir à jour la liste des « signatures » de virus. Cela doit être réalisé le plus souvent possible (idéalement tous les jours) et au moins une fois lors de chaque alerte importante (signalée par les médias ou les sites d'antivirus par exemple)
4.10. Surveillance / audit. Chaque CPAS connecté au réseau de la Banque carrefour doit organiser, au moins une fois tous les quatre ans, un audit[6] concernant la situation de la sécurité tant au niveau logique que physique.	Politique de contrôle de la sécurité	Tous les services concernés par la sécurité de l'information	Coût variable selon la nature de l'audit (physique et informati-que	Un à plusieurs jours selon l'importance des installations.	L'audit recherche ici, par l'écoute des intervenants et en procédant par recoupements, à déterminer les vulnérabilités logiques et physiques fondamentales qui existent au sein d'un C.P.A.S. donné. Le coût peut être limité en demandant à un autre conseiller en sécurité de CPAS de faire un audit interne dans son propre CPAS

[6] Il s'agit d'un audit où l'initiative et les efforts financiers y afférents émanent de l'institution même. L'audit ne doit pas être complet.