Communauté de communes Maurienne Galibier

Rapport d'audit de sécurité informatique RGPD - Critères obligatoires

Versions du document

Version	Objet de la révision	Auteur	Date
V1	Création du document	M. Narioo	17/09/2019

Mme Chantal CHAUMAZ	Directrice générale des services
Mme Christelle ANDOUCHE	Chargé de mise en conformité

Contacts COVATEAM

Philippe Dujardin	Directeur commercial	06 77 40 23 80	philippe.dujardin@covateam.com
Frédéric Léger	Directeur technique	06 82 72 09 62	frederic.leger@covateam.com
Mathieu Narioo	Consultant	06 11 43 21 00	mathieu.narioo@covateam.com

Rapport d'audit de sécurité informatique RGPD - Critères obligatoires

17 septembre 2019

Table des matières

Rapport d'audit de sécurité informatique RGPD - Critères obligatoires

17 septembre 2019

1 - Mission d'audit

1.1 - Contexte et objectifs de l'audit

La communauté de commune de Maurienne Galibier une grosse trentaine d'utilisateurs connectés, sur 6 sites :

1. Le siège avec 9 à 11 utilisateurs
2. Station d'épuration avec 3 utilisateurs
3. Maison de l'enfance avec 6 utilisateurs
4. Périscolaire en centre de loisir avec 8 utilisateurs
5. Périscolaire en centre de loisir Valloire avec 5 utilisateurs
6. Garage avec 2 utilisateurs

Plusieurs prestataires informatiques avec des fonctions différentes. Les actions de ces prestataires ne sont pas forcément maitrisées par le personnel interne de la communauté de communes.

- Magasin Maurienne Informatique pour l'achat de matériel et l'installation
- CDEG pour l'installation de la baie et câblage (et réseau ?)
- Neologik pour l'installation du firewall Zyxel
- Relation direct avec Intégrateur CEGID (Compta RH)
- Relation direct avec Défi informatique pour logiciel L&A (Périscolaire/cantine/ALSH)

Mme Christelle ANDOUCHE et Mme Chantal CHAUMAZ sont chargées de la mise en conformité au RGPD (juridique et technique) et a assisté à la 1ère journée de sensibilisation.

Les objectifs sont :

- Faire un audit de la sécurité informatique pour le contrôle de la conformité au RGPD, selon les critères de la CNIL. Cet audit ne remplace pas un audit approfondi ou global du système d'information.

- Proposer un plan d'action ou un portefeuille de projets adapté aux besoins.

1.2 - Périmètre de l'audit

L'audit est déroulé sur une journée et intègre les critères obligatoires de sécurité informatique tel que défini dans le guide de la sécurité personnelle [GSP] de la CNIL (09/2017).

Sont exclus les critères avancés du GSP ainsi que les autres référentiels sur la sécurité des systèmes d'information comme les normes ISO 27000, PCI-DSS, etc.

1.1 - Eléments à prendre en compte

1. Un espace publique ouvert à tous est présent dans les locaux afin de donnée un accès à des ordinateurs et internet. Il est nécessaire de sécuriser ces accès et de les dissocier du réseau de la ComCom. De plus il faudra valider les conditions de connexion et de surveillance à mettre en place pour des accès au public avec un service juridique

2. Les locaux de la comcom sont prêtés au mois de mai pour la foire aux plants et pour donner accès aux salles de réunion pour les élus. Il est donc encore plus nécessaire de sécuriser la zone informatique et de dissocier les différents réseaux de la Comcom.

1.2 - Organisation de l'audit

Le déroulement de l'audit se réalise avec les étapes suivantes :

Description	Objectif	Temps estimatif
Présentation de l'audit	Expliquer le périmètre, la méthodologie, les livrables.	0,5 h
Questionnaire des critères obligatoire	Evaluer pour chaque critère le niveau de conformité.	2 h
Complément d'information	Pour les critères dont les réponses ne sont pas suffisantes, recherche ou approfondissement.	2,5 h
Travail de synthèse de l'auditeur	Analyse des réponses et recommandations, rédaction du rapport.	1 h
Présentation du rapport	Principales conclusions, proposition de priorisation	1 h

2 - Conclusion de l'audit pour les décideurs

2.1 - Principaux points observés lors de l'audit

2.1.1 - Synthèse graphique et conclusion

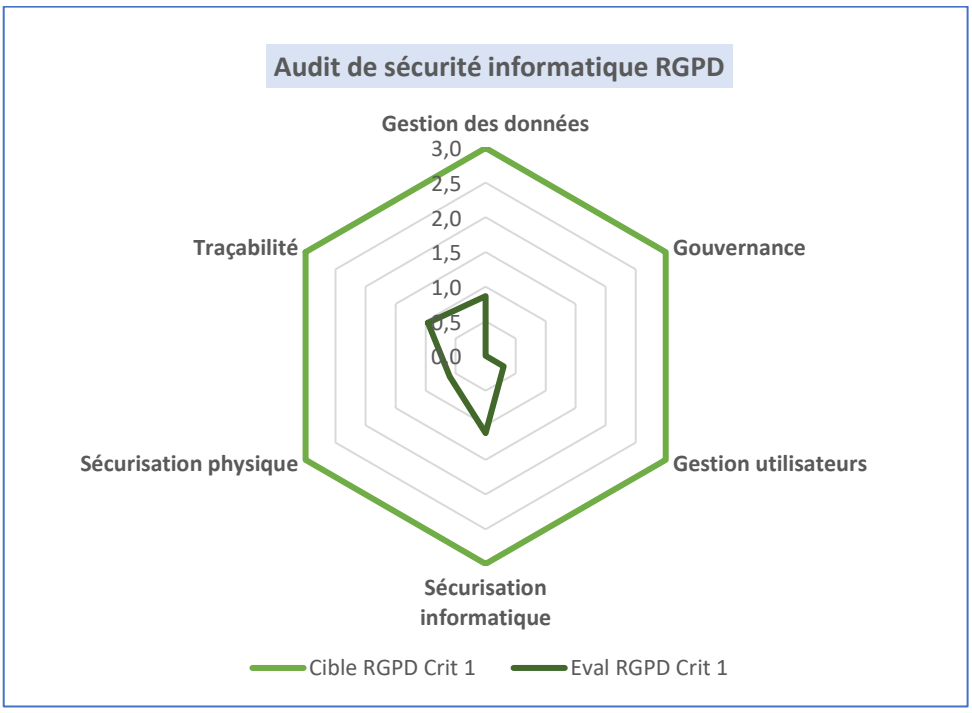
L'audit révèle des risques élevés dans tous les domaines audités. La mise en place des bonnes pratiques énoncées dans le questionnaire ci-dessous seront à mettre en œuvre dans les plus brefs délais. Tous les domaines doivent être pris en compte.

Les processus procédant de la gestion des utilisateurs (notée 0,3/3) et des données (notée 0,9/3) devront être créer et mis en place dans les plus brefs délais. L'accent est à mettre sur les bases de la sécurité informatiques en créant des comptes utilisateurs nominatifs avec politique de mot de passe, organisation des données sur un support type serveur ou NAS avec des règles d'habilitation d'accès aux données et un plan de sauvegarde et de reprise d'activité.

La gouvernance devra être mise en place en prenant contact avec l'ensemble des prestataires pour une mise à plat des contrats et la mise en place d'une maintenance informatique.

La traçabilité et la sécurisation physique notées respectivement 1/3, et 0,6/3 seront améliorée en suivant les recommandations présentes dans le questionnaire ci-dessous notamment en retirant les droits administrateurs aux utilisateurs, en améliorant la sécurité de la zone informatique et en vérifiant que les bureaux et armoires sont bien fermés à clefs.

La moyenne globale est de 0,6/3.



A noter que la sécurisation logiciel concerne les aspects autour des développements et des techniques cryptographiques associées. Aucun développement n'est effectué en interne, l'évaluation n'est donc pas à réaliser.

2.1.2 - Principaux points forts constatés

Les postes informatiques présentent un OS et une solution de sécurité (Bitdefender total security) à jour, par contre les utilisateurs sont administrateur des postes et la solution est monoposte et d'usage au particulier.

Deux NAS sont utilisés pour les sauvegardes.

Les interventions par les tiers sur le système d'information sont correctement encadrées.

2.1.3 - Principaux points faibles constatés

Les bases de la sécurité informatique sont absentes : Pas de compte utilisateur unique et nominatif sur la plupart des postes et sur certaines applications métiers, pas d'utilisation systématique de mot de passe ni de fermeture automatique des sessions et donc pas de politique de mot de passe sur les sessions utilisateurs.

Les mots de passe sont parfois notés dans des endroits accessibles (classeur, agenda,…)

Il n'y a pas de serveur de données, ni de NAS fonctionnel. Les données sont sur les postes de travail partagés à toutes les personnes reliées au réseau (filaire ou wifi public et privé). Il n'y a donc pas d'habilitation sur les données et un risque majeur de fuite d'informations. Le stockage des données de la comcom est non connu selon les utilisateurs (donnée sur poste perso, données sur poste partagé, Dropbox …).

Les sauvegardes paramétrées sont faites à l'utilisateur et non vérifiées. Aucune centralisation de la donnée n'est faite. Actuellement la comcom est en zone de risque très important en cas d'attaque virale et ou de sinistre majeur.

Pas d'existence d'une charte informatique contraignante. Il faut la mettre en place et la faire signer par l'ensemble des utilisateurs.

La comcom n'a pas de prestataire informatique attitré avec un contrat de maintenance annuel sur lequel s'appuyer.

Il n'y a pas d'archivage numérique existant.

Il n'y a pas d'alarme et la zone informatique n'est pas sécurisée.

La gestion de l'archivage devra être mis en œuvre.

Valider la sécurité informatique (utilisation du Zyxel, mise en place d'un filtrage URL,…)

Le site internet devra être mis à jour pour respecter la RGPD (bandeau de cookie, mentions légales et politique de confidentialité). Cf. https://www.poivre-et-sell.com/rgpd-cas-concret-mise-en-conformite/

La gouvernance devra être appliquée en reprenant l'ensemble de contrats avec les sous-traitants et les prestataires.

2.1.4 - Eléments du questionnaire sans réponse

Aucun.

2.2 - Proposition de plan d'action

QUOI	QUI	Criticité
Revoir l'infrastructure réseau pour séparer totalement les réseaux publics et privés. Actuellement les 2 réseaux se voient et se parlent.	CCGM /Presta	URGENTE
Sécuriser les partages sur les NAS et les PC utilisateurs pour que les accès aux données ne soient plus accessibles à tous	CCGM /Presta	URGENTE
Mettre en place des sessions nominatives et sécurisées sur l'ensemble des postes des utilisateurs grâce à l'utilisation du rôle Windows AD d'un serveur, Azure AD avec office 365, ou d'un NAS SYNOLOGY ou QNAP en fonction des sites.	CCGM /Presta	Très Haute
Mettre en place une politique de sécurité à jour (verrouillage auto, complexité des mots de passe, renouvellement de ces derniers 1x/an)	CCGM / Presta	Très Haute
Améliorer la sécurité des données en mettant en place soit un NAS, soit un serveur, soit une externalisation (O365 par ex) et créer des groupes pour gérer des habilitations d'accès. Suivre les habilitations avec un fichier Excel à revoir tous les ans.	CCGM / Presta	Haute
Mettre en place un plan de reprise d'activité avec sauvegarde 321 des données et systèmes + rétention sur 30j minimum et test de restauration avec un logiciel dédié comme VEEAM.	CCGM / Presta	Haute
Migrer toutes les messageries gmail, wanadoo et Orange vers un hébergement professionnel ou un abonnement Office 365 permettant de bénéficier de l'ensemble des fonctionnalités Outlook et plus. (Domaine maurienne-galibier.com et plus gmail.com ou wanadoo.fr)	CCGM / Presta	Haute
Comprendre l'environnement réseau avec pare feu matériel à jour et permettant le filtrage web. Vérifier l'éligibilité des connexions pour mise en place O365 et/ou VPN avec autre sites	CCGM / Presta	Haute
Sécuriser les équipements mobiles avec Bitlocker ou autres	CCGM	Haute
Mettre en place une charte informatique complète et contraignante, la faire signer par les utilisateurs	CCGM	Moyenne
Vérifier la conformité RGPD des prestataires	CCGM	Moyenne
Mettre en place de l'archivage numérique.	CCGM	Moyenne
Créer les procédures de déclaration de violation de données et de restitution/suppression de la donnée	CCGM	Moyenne

3 - Rapport détaillé de l'audit

3.1 - RGPD et critères obligatoires

3.1.1 - Thème gouvernance

N°	Questions	Note	Cible	Réponses
13.1	Prévoyez une clause spécifique dans les contrats des sous-traitants	0	5	Relancer les sous-traitants si pas reçu d'avenants au contrat.

13.2	Prévoyez les conditions de restitution et de destruction des données	0	5	Procédures à prévoir, à mettre en œuvre à l'aide des fournisseur d'application
13.3	Assurez-vous de l'effectivité des garanties prévues (audits de sécurité, visites, etc.)	0	5	Reprendre les contrats existants !
13.4	CE QU'IL NE FAUT PAS FAIRE : 1-Entamer la prestation de sous-traitance sans avoir signé un contrat avec le prestataire reprenant les exigences posées par l'article 28 du Règlement général sur la protection des données. 2-Avoir recours à des services de cloud sans garantie quant à la localisation géographique effective des données et sans s'assurer des conditions légales et des éventuelles formalités auprès de la CNIL pour les transferts de données en dehors de l'Union européenne.	0	5	1) A mettre en œuvre pour les futures consultations. 2) Ne pas le faire pour les données personnelles

3.1.2 - Thème gestion utilisateurs

N°	Questions	Note	Cible	Réponses
1.1	Informez et sensibilisez les personnes manipulant les données	2	5	Première information auprès des responsables des services. Plus transfert des fichers pour la récupération des traitements. Ne pas hésiter à faire une diffusion papier.
1.2	Rédigez une charte informatique et lui donner une force contraignante	0	5	A mettre en place. Prendre exemple sur internet.
2.1	Définissez un identifiant (login) unique à chaque utilisateur	1	5	Pas d'identifiant unique par personne sur PC. Compte parfois unique sur les logiciels. Créer des identifiants nominatifs uniques pour tous les utilisateurs à l'iade du service AD d'un contrôleur de domaine (serveur ou NAS) et logiciels métiers
2.2	Adoptez une politique de mot de passe utilisateur conforme à nos recommandations	0	5	Définir la politique et la mettre en place avec les prestataires. Déployer Keepass et expliquer aux utilisateurs la nécessité d'utiliser leur mot de passe.
2.3	Obligez l'utilisateur à changer son mot de passe après réinitialisation	2	5	Utilisateurs peuvent changer les mots de passe sur logiciel métiers. Penser à réinitialiser ses mots de passe une fois par an minimum
2.4	Limitez le nombre de tentatives d'accès à un compte	0	5	A mettre en place sur les PC et vérifier sur les plateformes métiers.
2.5	CE QU'IL NE FAUT PAS FAIRE : 1-Communiquer son mot de passe à autrui. 2-Stocker ses mots de passe dans un fichier en clair, sur un papier ou dans un lieu facilement accessible par d'autres personnes. 3-Enregistrer ses mots de passe dans son navigateur sans mot de passe	0	5	1. échange de mot de passe 2. classeur / carnet de mot de passe Mettre en place Keepass pour les utilisateurs.

	maître. 4-Utiliser des mots de passe ayant un lien avec soi (nom, date de naissance, etc.). 5-Utiliser le même mot de passe pour des accès différents. 6-Conserver les mots de passe par défaut. 7-S'envoyer par e-mail ses propres mots de passe.			
3.1	Définissez des profils d'habilitation	0	5	Fichiers sur les PC utilisateurs avec partage de dossier en public. Pas de centralisation, pas d'habilitation. Attention les données sont accessibles à partir du wifi public et sur les PC en libre-service. Mettre en place une centralisation des données avec un serveur de données ou un NAS, avec groupe de sécurité et gestion des habilitations.
3.2	Supprimez les permissions d'accès obsolètes	0	5	Faire un état des lieux avec la revue des habilitations. Créer des processus d'entrée / sortie des utilisateurs avec liste des accès à créer/supprimer.
3.3	Réaliser une revue annuelle des habilitations	0	5	A mettre en place à partir du fichier à créer.

3.1.3 - Thème gestion des données

N°	Questions	Note	Cible	Réponses
10.1	Effectuez des sauvegardes régulières	2	5	Actuellement sauvegarde bi-hebdomadaire des PC sur NAS (6 sauvegardes complètes conservées) avec Cobian Backup. Sauvegarde système mensuel pas toujours correctement effectuées. Pas de chiffrement, pas de sécurité car NAS accessible à tous même au wifi public.
10.2	Stockez les supports de sauvegarde dans un endroit sûr	2	5	Sauvegarde sur NAS sous l'escalier avec porte non fermée pour pb de chaleur
10.3	Prévoyez des moyens de sécurité pour le convoyage des sauvegardes	0	5	Pas concerné.
10.4	Prévoyez et testez régulièrement la continuité d'activité	2	5	Pas de test de restauration (pas de contrat de maintenance) mais récupération de fichier déjà effectuée.
10.5	CE QU'IL NE FAUT PAS FAIRE : Conserver les sauvegardes au même endroit que les machines hébergeant les données. Un sinistre majeur intervenant à cet endroit aurait comme conséquence une perte définitive des données.	2	5	Sauvegarde sur NAS sous l'escalier avec porte non fermée pour pb de chaleur

11.1	Mettez en œuvre des modalités d'accès spécifiques aux données archivées	2	5	Archivage papier dans entrepôt à côté de la gare. Mise en armoire dans zône sécurisée en cours. Voir pour se faire aider par le centre de gestion. Numérique : A mettre en place.
11.2	Détruisez les archives obsolètes de manière sécurisée	0	5	Mettre en place procédure d'archivage, suppression, anonymisation
11.3	CE QU'IL NE FAUT PAS FAIRE : 1-Utiliser des supports ne présentant pas une garantie de longévité suffisante. À titre d'exemple, la longévité des CD et DVD inscriptibles dépasse rarement 4/5 années. 2-Conserver les données en base active en les notant simplement comme étant archivées. Les données archivées ne doivent être accessibles qu'à un service spécifique chargé d'y accéder.	2	5	1- Pas concerné 2-pas d'archive pour le moment
12.1	Enregistrez les interventions de maintenance dans une main courante	0	5	Mettre en place un fichier Excel avec date et heure d'intervention + Nom du prestataire + motif de l'intervention par service avec pilotage par une personne.
12.2	Encadrez par un responsable de l'organisme les interventions par des tiers	5	5	Intervention encadrée par l'accueil. Valider que ok sur tous les sites.
12.3	Effacez les données de tout matériel avant sa mise au rebut	4	5	Procédure de destruction existante. Valider que les données sont bien détruites.
12.4	CE QU'IL NE FAUT PAS FAIRE : 1-Installer des applications pour la télémaintenance ayant des vulnérabilités connues, par exemple qui ne chiffrent pas les communications. 2-Réutiliser, revendre ou jeter des supports ayant contenu des données à caractère personnel sans que les données n'aient était supprimées de façon sécurisée.	2	5	Mettre à jour TeamViewer (V5 pour DEFI informatique !)
14.1	Chiffrez les données avant leur envoi	0	5	Attention à l'envoi des données par DEFI sur adresse email Gmail. Mettre en place une procédure pour sécuriser les données personnelles.
14.2	Assurez-vous qu'il s'agit du bon destinataire	0	5	Attention aux adresses emails globales.
14.3	Transmettez le secret lors d'un envoi distinct et via un canal différent	0	5	Mettre en place avec 7zip en envoi de SMS pour le mot de passe quand adresse globale
14.4	CE QU'IL NE FAUT PAS FAIRE : Transmettre des fichiers contenant des données personnelles en clair via des messageries grand public.	0	5	Attention à l'envoi vers des messageries Gmail, Hotmail,…

3.1.4 - Thème sécurisation informatique

N°	Questions	Note	Cible	Réponses

5.1	Prévoyez une procédure de verrouillage automatique de session	0	5	A mettre en place en place sur les PC. Communiquer sur le verrouillage manuel. Windows + L
5.2	Utilisez des antivirus régulièrement mis à jour	2	5	Bitdefender Total Security ! Solution de sécurité pour particulier. Passer à une version PRO.
5.3	Installez un « pare-feu » (firewall) logiciel	2	5	Bitdefender Total Security ! Solution de sécurité pour particulier. Passer à une version PRO.
5.4	Recueillez l'accord de l'utilisateur avant toute intervention sur son poste	5	5	Prise en main par TeamViewer avec demande de mot de passe.
5.5	CE QU'IL NE FAUT PAS FAIRE : 1-Utiliser des systèmes d'exploitation obsolètes. 2-Donner des droits administrateurs aux utilisateurs n'ayant pas de compétences en sécurité informatique.	3	5	1. Windows 7 et 10 2. Droit admin à retirer aux utilisateurs.
6.1	Prévoyez des moyens de chiffrement des équipements mobiles	0	5	Disque dur non chiffré. Smartphone non sécurisé. A mettre en place rapidement.
6.2	Faites des sauvegardes ou synchronisations régulières des données	3	5	Sauvegarde programmée sur certains portables. Voir avec le prestataire pour généraliser la sauvegarde sans action des utilisateurs
6.3	Exigez un secret pour le déverrouillage des smartphones	2	5	A vérifier sur tous les utilisateurs de smartphone.
7.1	Limitez les flux réseau au strict nécessaire	2	5	Boitier Zyxel USG60W installé. Pas de filtrage URL. Voir avec prestataire le paramétrage.
7.2	Sécurisez les accès distants des appareils informatiques nomades par VPN	5	5	Non concerné
7.3	Mettez en œuvre le protocole WPA2 ou WPA2-PSK pour les réseaux Wi-Fi	5	5	Wifi WPA2
7.4	CE QU'IL NE FAUT PAS FAIRE : 1-Utiliser le protocole telnet pour la connexion aux équipements actifs du réseau (pare-feu, routeurs, passerelles). Il convient d'utiliser plutôt SSH ou un accès physique direct à l'équipement. 2-Mettre à disposition des utilisateurs un accès Internet non filtré. 3-Mettre en place un réseau Wi-Fi utilisant un chiffrement WEP.	1	5	Mettre en place un filtrage sur l'accès internet.
8.1	Limitez l'accès aux outils et interfaces d'administration aux seules personnes habilitées	2	5	Pas de serveur en interne. Logiciel DEFI informatique en mode Saas. PC utilisateur pour serveur CEGID (compta et RH), à changer au plus vite.
8.2	Installez sans délai les mises à jour critiques	2	5	Mise à jour auto sur les postes. Pas d'information sur le NAS de sauvegarde.
8.3	Assurez une disponibilité des données	0	5	Données sur les postes des utilisateurs.

8.4	CE QU'IL NE FAUT PAS FAIRE : 1-Utiliser des services non sécurisés (authentification en clair, flux en clair, etc.). 2-Utiliser pour d'autres fonctions les serveurs hébergeant les bases de données, notamment pour naviguer sur des sites web, accéder à la messagerie électronique, etc. 3-Placer les bases de données sur un serveur directement accessible depuis Internet. 4-Utiliser des comptes utilisateurs génériques (c'est-à-dire partagés entre plusieurs utilisateurs).	0	5	Pas de serveur alors que nécessaire.
9.1	Utilisez le protocole TLS et vérifiez sa mise en œuvre	0	5	Site en http. Rapport SSL site SSLAB : F. Demander la mise en place de la sécurité du site.
9.2	Vérifiez qu'aucun mot de passe ou identifiant ne passe dans les url	5	5	OK pas de pb
9.3	Contrôlez que les entrées des utilisateurs correspondent à ce qui est attendu	0	5	Formulaire non sécurisé, à revoir. Test des champs numéro et vérification adresse email + captcha pour bloquer les robots.
9.4	Mettez un bandeau de consentement pour les cookies non nécessaires au service	0	5	Pas de bandeau de cookie, pas de politique de confidentialité. A mettre à jour rapidement.
9.5	CE QU'IL NE FAUT PAS FAIRE : 1-Faire transiter des données à caractère personnel dans une URL telles que identifiants ou mots de passe. 2-Utiliser des services non sécurisés (authentification en clair, flux en clair, etc.). 3-Utiliser les serveurs comme des postes de travail, notamment pour naviguer sur des sites web, accéder à la messagerie électronique, etc. 4-Placer les bases de données sur un serveur directement accessible depuis Internet. 5-Utiliser des comptes utilisateurs génériques (c'est-à-dire partagés entre plusieurs utilisateurs).	0	5	Voir avec le prestataire informatique

3.1.5 - Thème sécurisation logiciel

N°	Questions	Note	Cible	Réponses
16.1	Proposez des paramètres respectueux de la vie privée aux utilisateurs finaux	0	5	*non concerné*
16.2	Évitez les zones de commentaires ou encadrez-les strictement	0	5	*non concerné*
16.3	Testez sur des données fictives ou anonymisées	0	5	*non concerné*

16.4	CE QU'IL NE FAUT PAS FAIRE : 1-Utiliser des données à caractère personnel réelles pour les phases de développement et de test. Des jeux fictifs doivent être utilisés autant que possible. 2-Développer une application puis réfléchir dans un second temps aux mesures de sécurité à mettre en place.	0	5	*non concerné*
17.1	Utilisez des algorithmes, des logiciels et des bibliothèques reconnues	0	5	*non concerné*
17.2	Conservez les secrets et les clés cryptographiques de manière sécurisée	0	5	*non concerné*
17.3	CE QU'IL NE FAUT PAS FAIRE : 1-Utiliser des algorithmes obsolètes, comme les chiffrements DES et 3DES ou les fonctions de hachage MD5 et SHA1. 2-Confondre fonction de hachage et chiffrement et considérer qu'une fonction de hachage seule est suffisante pour assurer la confidentialité d'une donnée. Bien que les fonctions de hachages soient des fonctions « à sens unique », c'est à dire des fonctions difficiles à inverser, une donnée peut être retrouvée à partir de son empreinte. Ces fonctions étant rapides à utiliser, il est souvent possible de tester automatiquement toutes les possibilités et ainsi de reconnaître l'empreinte.	0	5	*non concerné*

3.1.6 - Thème sécurisation physique

N°	Questions	Note	Cible	Réponses
15.1	Restreignez les accès aux locaux au moyen de portes verrouillées	3	5	Bureaux avec portes extérieures verrouillées en dehors des heures d'ouverture. Données RH et comptable dans armoire sous clef. Attention aux oublis.
15.2	Installez des alarmes anti-intrusion et vérifiez-les périodiquement	0	5	Pas d'alarme.
15.3	CE QU'IL NE FAUT PAS FAIRE : Sous-dimensionner ou négliger l'entretien de l'environnement des salles informatiques (climatisation, onduleur, etc.). Une panne sur ces installations a souvent comme conséquence l'arrêt des machines ou l'ouverture des accès aux salles (circulation d'air) neutralisant de facto des éléments concourant à la sécurité physique des locaux.	0	5	Zône informatique sous l'escalier sans climatisation et onduleur non connecté.

3.1.7 - Thème Traçabilité

N°	Questions	Note	Cible	Réponses
4.1	Prévoyez un système de journalisation	2	5	Seul les Journaux Windows et les applications métiers sont ok. Attention utilisateur administrateur des postes.
4.2	Informez les utilisateurs de la mise en place du système de journalisation	0	5	A indiquer dans la charte informatique.
4.3	Protégez les équipements de journalisation et les informations journalisées	1	5	OK sur application métiers. Supprimer les droits administrateurs sur les postes.
4.4	Prévoyez les procédures pour les notifications de violation de données à caractère personnel	0	5	à prévoir pour notification sur site de la CNIL
4.5	CE QU'IL NE FAUT PAS FAIRE : Utiliser les informations issues des dispositifs de journalisation à d'autres fins que celles de garantir le bon usage du système informatique (par exemple, utiliser les traces pour compter les heures travaillées est un détournement de finalité, puni par la Loi).	5	5	RAS