

RISQUES CYBER - CDCA

Etablissement : Centre Jean-Marie LARRIEU

I. DONNEES GENERALES

Nombre total de personnes accueillies ou suivies : 125

Nombre total de salariés, tout statut confondu : 100

Budget d'Exploitation 2025 (*Dépenses de Fonctionnement*) : 5 471 730

Nombre de salariés utilisant le système d'information de l'entreprise : 100 + 100 usagers

Nombre de pc : 100

Nombre de serveur (IT) : 6 Physiques, 24 VM

Travaillez-vous avec un prestataire en sécurité informatique ? OUI ☒ NON ☐

Si OUI, précisez le nom de ce prestataire : Gestion hybride sécurisée : Pilotage stratégique et opérationnel assuré en interne par un RSI/RSSI dédié au CJML, appuyé par le prestataire ALLEO pour le support de second niveau sur l'infrastructure périmétrique (Pare-feu Fortinet) et la fourniture des solutions de sécurité.

1. Quels types de données à caractère personnel stockez-vous dans votre système d'information :

☒ Administratives

☒ Santé

☒ Bancaires

☐ Autres.....

2. Vos données sont-elles hébergées chez un tiers hébergeur ? OUI ☒ NON ☐

❓ Si OUI, lequel ? Le CJML s'appuie sur une architecture hybride et sectorisée pour maximiser la sécurité de ses données :

Infrastructure Locale Maîtrisée (On-Premise) : Par choix stratégique de souveraineté, nos données cœur de métier les plus sensibles — le Dossier Usager Informatisé (DUI Imago) et la Comptabilité publique — sont hébergées sur nos serveurs internes, isolées sur des VLAN dédiés et protégées par un pare-feu Fortinet.

Solutions SaaS Tiers (Cloud) : Notre solution de Gestion des Ressources Humaines et de Paie est externalisée chez l'éditeur spécialisé Numih (Hébergement sécurisé). Notre suite bureautique et de communication (e-mails, documents de travail) est portée par Google Workspace, configurée avec une localisation stricte du stockage des données au sein de l'Union Européenne (UE/EEE) et entièrement supervisée via notre console de gestion MDM. »

II. UTILISATEURS :

Chaque salarié dispose d'un identifiant (login) personnel et unique, nécessaire pour l'utilisation des appareils fixes ou mobiles OUI ☒ NON ☐

L'entreprise impose l'utilisation de mots de passe personnels et complexes : au moins 8 caractères d'au moins 2 types différents (*chiffres, majuscules, minuscules ...*) OUI ☒ NON ☐

Le nombre d'essais de saisie du mot de passe est limité à 5 tentatives au maximum : OUI ☒ NON ☐

3. **Procédez-vous à des formations et/ou sensibilisations de l'ensemble de votre personnel aux bonnes pratiques informatiques ?** OUI ☒ NON ☐

Si OUI, à quelle fréquence ? Campagne de Sensibilisation du GRADeS e-santé annuelle avec rappel mensuel sur la période de campagne et environ 3 test de phishing

4. **Vos collaborateurs sont-ils sensibilisés aux risques numériques et à leurs conséquences ?**
Plusieurs réponses possibles

- Des simulations d'attaques par phishing (hameçonnage) ? OUI ☒ NON ☐

- Des formations présentiels ou e-learning ? OUI ☒ NON ☐

- La diffusion de guide de bonnes pratiques ? OUI ☒ NON ☐

5. **Avez-vous mis en place une politique ou une charte de sécurité informatique formalisée, pilotée et régulièrement communiquée à l'ensemble de vos collaborateurs**
OUI ☒ NON ☐

III. SYSTEME INFORMATIQUE :

6. **Utilisez-vous un antivirus payant, à jour et dont la licence est en cours de validité ?**
OUI ☒ NON ☐

OUI. Le CJML déploie une stratégie de protection cyber active, payante et à jour, articulée autour d'une **micro-segmentation réseau stricte et d'une inspection globale des flux** :

1. **Protection Périmétrique & Wi-Fi (Fortinet)** : L'ensemble de notre infrastructure réseau — incluant le Wi-Fi d'entreprise et le Wi-Fi public — est intégralement filtré et protégé à la racine par les licences de sécurité annuelles actives (Bundle complet incluant Antivirus de flux, IPS et Filtrage applicatif) de notre pare-feu Fortinet. Cette protection s'applique de

manière universelle à tout appareil connecté (Chromebooks, smartphones, tablettes), sécurisant les flux web et neutralisant les menaces avant qu'elles n'atteignent les terminaux.

2. **Micro-Segmentation (VLANs)** : Pour éliminer le risque de propagation d'un logiciel malveillant (mouvement latéral), le SI est rigoureusement cloisonné en une vingtaine de VLANs étanches. Les environnements critiques (Serveurs locaux du DUI Imago et de la Comptabilité et infra support), les accès administratifs, les flux pédagogiques des usagers et les réseaux Wi-Fi sont totalement isolés les uns des autres.
3. **Sécurité Cloud (Google Workspace)** : Notre messagerie et nos documents de travail bénéficient du plus haut niveau de protection collaborative grâce aux licences payantes de notre suite **Google Workspace Education Plus** (anti-phishing algorithmique et analyse dynamique des pièces jointes).

7. **Avez-vous déployé un Endpoint Protection and Response (EDR) ?** OUI ☒ NON ☐

Oui, protection de niveau supérieur intégrée : terminaux ChromeOS durcis (Sandbox native par conception) managés par MDM Google, flux web sécurisés par ESET, serveurs Windows isolés sur VLAN dédié et protégés par les licences de sécurité actives (Bundle AV/IPS/Filtrage) de notre infrastructure de pare-feu Fortinet

8. **L'option firewall de vos postes de travail est-elle activée ?**

OUI ☒ NON ☐ Ne Sait ☐

9. **Avez-vous des outils de filtrage réseau sur votre système informatique ?**

OUI ☒ NON ☐ Ne Sait ☐

10. **Avez-vous un site internet ou un extranet ?**

OUI ☒ NON ☐

Si OUI :

- Le contrat d'hébergement de votre site intègre-t-il une solution anti-DDoS ?

OUI ☒ NON ☐

- Votre site est-il un point d'accès pour vos salariés et/ou vos partenaires ?

OUI ☐ NON ☒

- Votre site intègre-t-il des services de vente de produits et/ou de services en ligne ?

OUI ☐ NON ☒

🔍 **Si OUI** à cette question, répondre aux questions suivantes :

- Votre site internet est-il sécurisé via un protocole HTTPS ?

OUI ☒ NON ☐

- Conservez-vous les données bancaires de vos clients ou fournisseurs ?

OUI ☐ NON ☒

- Etes-vous référencé comme sous-traitant / fournisseur dans des grandes entreprises ou des administrations ?

OUI ☐ NON ☒

11. **Déterminez-vous des informations soumises à une obligation de confidentialité renforcée** (*secret des affaires, secret professionnel ou secret médical*) dans votre système informatique ?
- OUI ☒ NON ☐
- ☐ Si OUI à cette question, répondre à la question suivante :
- Ces informations concernent-elles des tiers (par exemple, vos clients, vos sous-traitants ou vos fournisseurs...) ?
- OUI ☒ NON ☐
12. **L'entreprise a mis en place une procédure de mise à jour au moins trimestrielle des systèmes d'exploitation, des logiciels bureautiques, des navigateurs et autres logiciels** (*notamment pour corriger les failles de sécurité*)
- OUI ☒ NON ☐
13. **Procédez-vous à la mise à jour des correctifs de sécurité** (*système d'exploitation et applications*) dans les 90 jours suivant leur publication officielle sur des sites de confiance ?
- OUI ☒ NON ☐
14. **L'entreprise fait appel à un prestataire d'audit de la sécurité des systèmes d'information qualifié ANSSI pour réaliser annuellement des tests d'intrusion ?**
- OUI ☐ NON ☒
- ☐ Si OUI, l'entreprise met systématiquement en œuvre les recommandations issues de ces tests :
- OUI ☐ NON ☐
15. **Disposez-vous d'une procédure de gestion des mots de passe ?**
- OUI ☒ NON ☐
16. **Les mots de passe sont-ils modifiés tous les 3 mois au maximum ?**
- OUI ☐ NON ☒
- L'ANSSI elle-même ne recommande plus cette pratique contre productive si le mot de passe est fort et d'autres mesures sont mises en place.
17. **Procédez-vous à une sauvegarde quotidienne de l'ensemble de vos données hors des sites d'origine ou d'exploitation** (*lieu sécurisé*) ?
- OUI ☒ NON ☐
- ☐ Si NON, fréquence :
- OUI (Architecture de résilience hybride et croisée avec externalisation planifiée).** Le CJML applique une stratégie de sauvegarde à 360° hautement sécurisée. Le périmètre Cloud (Google Workspace, RH Numih) fait l'objet de sauvegardes natives hors site gérées par les éditeurs. L'ensemble des données critiques *On-Premise* (DUI Imago, Comptabilité publique) ainsi que l'intégralité de notre environnement Cloud (*Google Workspace*) sont sauvegardés quotidiennement sur un NAS professionnel principal (Synology RS2424RP+).
- Pour parer aux risques de sinistre physique, ce volume global est répliqué en temps réel sur un second NAS (RS2424+) géographiquement isolé dans une zone distincte du campus, protégée par des murs coupe-feu en béton haute densité (bâtiment de conception hospitalière). Ce dispositif de continuité sera physiquement délocalisé hors site, sur notre implantation secondaire de Lannemezan, dès la finalisation du raccordement fibre optique actuellement en cours de déploiement. »

18. Comment les sauvegardes de l'ensemble des données nécessaires à votre activité sont-elles effectuées ?

Plusieurs réponses possibles :

☒ Sur des services sur internet configuré pour réaliser des sauvegardes en ligne (ex : cloud) ? OUI ☒ NON ☐

☒ Sur des supports déconnectés des postes informatiques ? OUI ☒ NON ☐

OUI (Isolation logique et immuabilité multi-périmètres). Nos serveurs de sauvegarde Synology sont totalement étanches vis-à-vis du réseau des utilisateurs et des Chromebooks (aucun partage réseau direct ou droit d'écriture n'est exposé aux terminaux).

La protection anti-ransomware est active et configurée via des politiques de *snapshots* immuables (clichés instantanés verrouillés en lecture seule). Ce mécanisme garantit la possibilité de restaurer instantanément et à une date antérieure non seulement nos bases de données locales (DUI), mais également l'historique complet de notre suite collaborative Google Workspace en cas d'attaque par rançongiciel ou de compromission de compte Cloud.

19. L'accès depuis des réseaux externes aux applicatifs et données internes se fait-il obligatoirement en utilisant une connexion VPN ou de niveau de sécurité équivalent ?

OUI ☒ NON ☐

20. Avez-vous recours à une Authentification multifacteurs (MFA) pour l'accès à distance au réseau et l'accès à la messagerie Web ?

OUI ☐ NON ☒

NON (Approche sectorisée : Protection par mot de passe durci sur le Web et contrôle matériel MDM sur le Réseau).

Le CJML fait le choix d'une transparence absolue : le MFA par code ou application n'est pas déployé à ce jour pour les utilisateurs standards en raison de contraintes d'exploitation médico-sociales. Il est en revanche **strictement obligatoire sur tous les comptes d'administration critiques**.

Pour sécuriser les deux périmètres visés, l'établissement applique deux politiques distinctes :

1. **Pour la messagerie Web (Google Workspace) :** L'accès est protégé par une politique de mots de passe robuste exigeant 12 caractères minimum, le respect de 3 critères de complexité, et un renouvellement obligatoire tous les 13 mois (afin de privilégier le cycle année scolaire).
2. **Pour l'accès à distance au Réseau (VPN) :** La configuration technique et les paramètres d'accès au pare-feu sont complexes, confidentiels et totalement masqués aux utilisateurs. Ce profil VPN est **exclusivement partagé et injecté à distance via notre console MDM (Google Admin)** sur les seuls équipements de l'établissement dûment autorisés. Par conséquent, le vol de simples identifiants réseau sur internet est insuffisant pour s'introduire dans le SI : un attaquant externe ne disposera jamais des paramètres secrets du VPN, qui restent confinés dans la boucle technique de nos terminaux managés.

21. Disposez-vous d'un Plan de Secours Informatique (PSI) et d'un Plan de Continuité d'Activité

(PCA) intégrant des scénarii liés à un incident de cyber-sécurité ? OUI ☒ NON ☐

(Procédures opérationnelles validées). Le CJML dispose de procédures de continuité d'activité en mode dégradé (continuité des soins et de l'accompagnement médico-social sur support physique/papier). Le Plan de Secours Informatique (PSI) cyber-spécifique, détaillant les procédures techniques de restauration à partir de nos snapshots Synology immuables, est actuellement en phase finale de formalisation documentaire.

22. Les sauvegardes de données sensibles ou à caractère personnel sont-elles systématiquement cryptées ? OUI ☒ NON ☐

Conformément aux recommandations de l'ANSSI et aux exigences du RGPD sur les données de santé, l'ensemble des sauvegardes du CJML est systématiquement **chiffré** (et non "crypté").

IV. ANTECEDENTS :

23. Êtes-vous actuellement assuré contre le risque CYBER ? OUI ☒ NON ☐

24. Avez-vous au cours des 3 dernières années été victime d'une cyber-attaque ?

OUI ☐ NON ☒

☒ Si OUI, nature de l'attaque :.....
Préjudice financier :.....

25. Avez-vous au cours des 3 dernières années été victime d'une violation des données personnelles ? OUI ☐ NON ☒

Si OUI, Préjudice financier :.....
