Création et rédaction d'une ébauche (squelette) de mise en œuvre de la sécurité physique dans un Système Informatique de production sécurisé d'une TPE.

Sur une architecture de production informatique très simple et courante, veuillez faire une proposition au **mieux disant** d'un système **fonctionnel et réaliste** de mise en place d'une sécurité physique du parc informatique et des locaux. A l'heure actuelle il n'existe pas de charte informatique interne à la société.

Définition du Parc de la société

Matériel fixe

- 3 ordinateurs type Workstation sous Windows 10 en réseau type Workgroups avec Windows Defender activé et paramétré
- 1 NAS double baie avec 2 HD de 4 To qui sert de serveur de fichiers et de stockage des sauvegardes en local.
- 1 HD externe 1 To pour sauvegardes légales et externes
- 1 connexion internet ADSL 2+ via un FAI lambda protégée par un Firewall type ZyXEL USG 40 + VPN + Protection AV native
- Une imprimante en réseau type HP Color LaserJet Pro MFP utilisée aussi pour faire de la GED des factures et les lier au CRM ou à Azure via le logiciel M-Files Cloud

Matériel nomade

- 1 ordinateur portable avec un Dock de connexion au réseau local ou une connexion 4G en déplacement avec accès sécurisé via un VPN et un AV type Suite Kasperky
- 2 tablettes numériques 10 pouces sous Android pour faire des démonstrations commerciales.
- 1 Vidéoprojecteur home cinéma LG HF85LSR Wifi Intégré, Miracast, DLNA, Bluetooth, Port Ethernet
- Les 5 personnes travaillant dans la TPE ont tous un smartphone sous Android à la fois personnel et professionnel.

Parc Logiciel

- 1 Abonnement au Cloud Azure pour sauvegardes externes
- La société utilise un CRM type Dolibarr et un site institutionnel de la société sous un CMS type Wordpress en ligne chez un Hébergeur en serveur dédié avec bases de données MySQL, les sauvegardes sont gérées sur le serveur dédié, l'espace FTP mis à disposition par l'hébergeur ainsi que rapatriées en local sur le NAS.
- Un des postes à la suite Adobe installée et gère le site internet de la société créé via un CMS en ligne chez un Hébergeur en serveur dédié avec bases de données MySQL, les sauvegardes sont gérées sur le serveur dédié, l'espace FTP mis à disposition par l'hébergeur ainsi que rapatriées en local sur le NAS.
- Un logiciel de comptabilité EBP Comptabilité installé sur un poste qui utilise MS SQL Express comme gestionnaire de base de données
- Tous les postes ont un Office 365 installé via une licence entreprise avec accès au Cloud Azure
- Les sauvegardes sont paramétrées et gérées par un applicatif Ashampoo Backup Plus

Vincent Draghi TP n° 3 (Activité à distance du 07/05/2020)

Configuration des locaux

- Local situé dans une zone économique à l'écart des habitations avec une fourniture d'électricité régulée
- 1 Parking devant le local
- Une entrée avec comptoir d'accueil 1 fenêtre et une porte avec volets roulants manuels, l'imprimante et la ligne fixe téléphonique
- 2 bureaux avec 2 postes Workstation sous Windows 10 avec 2 fenêtres avec volets roulants manuels
- 1 bureau direction avec 1 fenêtre avec volet roulant manuel avec un dock de connexion pour le portable
- 1 Espace de restauration interne avec 1 fenêtre avec volet roulant manuel avec 1 évier, 1 Micro-Onde, 1 cafetière, 1 réfrigérateur, 1 table et 6 chaises
- 1 Local technique sans ouverture extérieure avec le Firewall, le modem ADSL 2+, une mini baie de brassage avec un hub 16 ports, le NAS, le matériel nomade et le compteur électrique avec son tableau
- 1 Local aveugle avec WC et lavabo

APPRECIATION DU RISQUE PHYSIQUE

Catégorie de menace	Scénario de risque	Profil	Positionnement	Nature	Moyens techniques des attaquants
Infraction et espionnage	Mise en place d'un keylogger et d'une backdoor	Pirates, concurrents	Externe	Malveillance	Moyens
Vol	Vol des backups et des disques durs	Pirates, concurrents	Externe	Malveillance	Moyens

Evènements naturels	Incendie dans le local technique	Surchauffe d'un composant informatique	Interne	Accident	N/A
Pannes et interruptions matérielles	Coupure de courant	Défaillance du système électrique	Interne / Externe	Accident	N/A

ANALYSE D'IMPACT LIEE AUX RISQUES PHYSIQUES

Scénario de risque	Vulnérabilité	Vraisemblance (Peu vraisemblable, Vraisemblable, Très vraisemblable, Quasi Certain)	Gravité de l'impact (mineure, significative, Grave, Critique)	Conséquences	Acceptabilité du risque (Acceptable en l'état, Tolérable sous contrôle, innaceptable
A. Mise en place d'un keylogger et d'une backdoor	Accès aux bureaux et le local technique non protégés	Très vraisemblable	Grave	Cout important. Perte de confiance clients, défiance des actionnaires	Innaceptable

				et des partenaires, risques pénales (violation RGPD…)	
B. Vol des backups et des disques durs	Accès au local technique non protégé et aucun contrôle des personnes habilitées	Très vraisemblable	Critique	Cout important. Perte de confiance clients, défiance des actionnaires et des partenaires, risques pénales (violation RGPD…)	Innaceptable
C. Incendie dans la salle des serveurs	Mauvaise ventilation du NAS et la mini baie de brassage	Peu vraisemblable	Critique	Destruction du matériel et des données clients	Innaceptable
D. Coupure de courant	Pas de générateurs de secours ni de onduleurs.	Vraisemblable	Grave	Interruption de l'activité et du travail réalisé si absence de sauvegardes	Innaceptable

Evaluation du risque

Vraisemblance	Quasi certain			**A**	
	Très vraisemblable				**B**

	Vraisemblable			**D**	
	Peu vraisemblable				**C**
		Mineure	Significative	Grave	Critique
		Gravité			

Ebauche de mise en œuvre de la sécurité physique

Biens	Clause ISO 27001
• 1 ordinateur portable : Dock de connexion au réseau local / connexion 4G via VPN + Suite Kasperky • 1 HD externe 1 To • 2 tablettes numériques 10 pouces (Android) • 1 Vidéoprojecteur LG HF85LSR (Wifi, Miracast, DLNA, Bluetooth, Ethernet) • 5 smartphones pro et perso (Android)	A.6.2.1 A.8.3.1

Catégorie de contrôle / Mesure	Contrôle / Mesure
Appareils mobiles et télétravail	Assurer la sécurité du télétravail et de l'utilisation d'appareils mobiles
Gestion des supports amovibles	Mettre en œuvre des procédures de gestion des supports amovibles conformément au plan de classification adopté par l'organisation.

Mise en œuvre

- Référencement des appareils mobiles sur un document via office 365 (voir le tableau suivant sur l'inventaire des actifs)
- Antimalware : harmoniser la protection des 5 smartphones professionnels, l'ordinateur portable et les 2 tablettes avec la Suite Kasperky installé sur tous les supports.
- Restrictions : comptes utilisateurs avec nécessité d'avoir un une habilitation type administrateur pour installer des logiciels.
- Verrouillage du dock sur le bureau avec des câbles antivol. Armoire verrouillée pour entreposer les appareils avec clefs gardées par le responsable.
- Authentification : Si le portable est équipé d'un lecteur de carte, usage de ce dernier avec la carte à puce. A défaut, accès des appareils se font avec mot de passe (8 chiffres minimum alphanumériques avec caractères spéciaux). (l'usage de Cisco Duo Security ou l'authentification multifacteur Azure pour du MFA semble disproportionné en raison des tarifs de ces solutions)
- Restrictions liées aux connexions à des services d'information : connexion via VPN et blocage des sites/flux via une politique de filtrage « deny by default » par le pare-feu ZyXEL USG 40
- Vidéoprojecteur : Usage de WPA2 avec changement de mot de passe (8 chiffres minimum alphanumériques avec caractères spéciaux) tous les 6 mois. Désactiver en fin d'usage. Désactiver par défaut les fonctionnalités jamais utilisées tel que Bluetooth ou Miracast.
- Désactivation, effacement des données ou verrouillage à distance (à voir selon les paramètres)

- Smartphones : Achat de 5 smartphones professionnelles neufs + formatage bas niveau à la première utilisation.
- Sauvegardes : hebdomadaires en local vers le NAS + cloud Azure
- Crypter l'ordinateur portable et les 2 tablettes en cas de vol (Bitlocker pour le portable et activation des paramètres pour Android)
- Ne permettre l'accès aux informations de l'organisation que lorsque l'utilisateur a signé un contrat d'utilisateur final par lequel il prend acte de ses missions (protection physique, mise à jour des logiciels, etc.), renonce à la propriété des données de l'organisation et autorise l'entreprise à effacer ses données à distance en cas de perte ou de vol de l'appareil, ou lorsque son utilisation n'est plus autorisée.
- Formation et sensibilisation : Courte formation d'un après-midi sur les bonnes pratiques pour l'usage des outils mobiles et les nouveaux dispositifs de sécurité. Rappels plusieurs fois par an.
- Partage du risque : Vérifier si l'assurance de l'entreprise prend en charge la destruction, vol des appareils.
- Limiter les risques liés à la dégradation du support : lorsque les données stockées sont encore nécessaires, transférer de ces données sur un support neuf, avant qu'elles ne deviennent illisibles pour le disque dur externe HD 1TO vers un autre support amovible.
- Activer le disque dur externe que lorsque nécessaire et lorsqu'il est nécessaire d'utiliser ce dernier, il convient de contrôler le transfert de l'information sur ces supports. A inclure dans la charte informatique à réaliser.

Biens	Clause ISO 27001
• Matériels : (3 ordinateurs, 1 NAS, 1 HD externe, Firewall, Imprimante HP, 1 ordinateur portable + Dock, 2 tablettes	A.8.1.1 A.8.1.2

numériques, 1 vidéoprojecteur, 5 smartphones android, locaux et fournitures, parking…) • Immatériels : (Abonnement Cloud Azure, CRM Dolibarr, BDO MySQL, CMS en ligne, suite Adobe, EPB comptabilité, office 365, Ashampoo Backup plus)	A.8.1.3 A.8.1.4
Catégorie de contrôle / Mesure	**Contrôle / Mesure**
Inventaire des actifs	Il convient d'identifier les actifs associés à l'information et aux moyens de traitement de l'information et de dresser et tenir à jour un inventaire de ces actifs.
Propriété des actifs	Il convient que les actifs figurant à l'inventaire aient un propriétaire.
Utilisation correcte des actifs	Il convient d'identifier, de documenter et de mettre en œuvre des règles d'utilisation correcte de l'information, des actifs associés à l'information et des moyens de traitement de l'information.
Restitution des actifs	Il convient que tous les salariés et utilisateurs tiers restituent la totalité des actifs de l'organisation qu'ils ont en leur possession au terme de la période d'emploi, du contrat ou de l'accord.
Mise en œuvre	

- Répertorier l'ensemble des actifs et Identifier les actifs les plus important pour la TPE (en priorisant les données et la protection du personnel). Vu l'absence d'une CMBD ou d'outils de gestion de parc, des fiches d'inventaires suffisent via Office 365 + copie sur le NAS.
- Chaque actif inventorié aura un propriétaire qui sera chargé de classer et protéger le/les actifs attribués. S'appuyer sur un modèle RACI est possible.
- Définir et revoit périodiquement les classifications et les restrictions d'accès aux actifs importants, en tenant compte des politiques de contrôle d'accès applicables;
- Inclure dans la charte informatique (à réaliser), une utilisation appropriée des biens
- Formaliser le processus de fin de mission ou d'emploi et inclure la restitution de tous les actifs physiques et électroniques. Enlever les droits pour accéder aux logiciels,OS, wi-fi.
- S'assurer que les manipulations de suppression ou de destruction des actifs sont réalisées correctement. Pour les disques durs : démagnétisation avec un dégaussage puis destruction physique.

Note : Ces mesures concernent autant la sécurité physique que logique.

Biens	Clause ISO 27001
• Matériel : (3 ordinateurs, 1 NAS, 1 HD externe, Firewall, Imprimante HP, 1 ordinateur portable + Dock, 2 tablettes numériques, 1 vidéoprojecteur, 5 smartphones android, locaux et fournitures, parking…)	A.9.1.1 A.9.2.1 A.9.2.2 A.9.2.3 A.9.2.4

• Immatériel : (Abonnement Cloud Azure, CRM Dolibarr, BDO MySQL, CMS en ligne, suite Adobe, EPB comptabilité, office 365, Ashampoo Backup plus)	A.9.2.5 A.9.2.6
Catégorie de contrôle / Mesure	**Contrôle / Mesure**
Politique de contrôle d'accès	Etablir, de documenter et de revoir une politique du contrôle d'accès sur la base des exigences métier et de sécurité de l'information.
Enregistrement et désinscription des utilisateurs	Mettre en œuvre une procédure formelle d'enregistrement et de désinscription des utilisateurs destinée à permettre l'attribution de droits d'accès.
Maîtrise de la gestion des accès utilisateur	mettre en œuvre un processus formel de maîtrise de la gestion des accès utilisateur pour attribuer ou révoquer des droits d'accès à tous les types d'utilisateurs de tous les systèmes et de tous les services d'information. restreindre et de contrôler l'attribution et l'utilisation des privilèges d'accès.
Gestion des privilèges d'accès	Il convient que l'attribution des informations secrètes d'authentification soit réalisée dans le cadre d'un processus de gestion formel.

Gestion des informations secrètes d'authentification des utilisateurs	Il convient que l'attribution des informations secrètes d'authentification soit réalisée dans le cadre d'un processus de gestion formel.
Revue des droits d'accès utilisateur	Il convient que les propriétaires d'actifs revoient les droits d'accès des utilisateurs à intervalles réguliers.
Suppression ou adaptation des droits d'accès	Il convient que les droits d'accès de l'ensemble des salariés et utilisateurs tiers à l'information et aux moyens de traitement de l'information soient supprimés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat ou de l'accord.

Mise en œuvre

- Formaliser et détailler les contrôles d'accès à la fois logiques et physiques : procédure d'accès au site selon les horaires de travail, passer par le bureau d'accueil pour accéder aux autres pièces de l'entreprise (ne pas passer par une porte de secours), port de la carte d'identification avec photo autour du cou, procédure spécifique pour le public étranger tel que les clients qui viennent sur les locaux de l'entreprise…
- Création d'identifiants utilisateurs uniques permettant de relier les utilisateurs à leurs actions et de les leur imputer. Exemple : création de profils utilisateurs uniques pour chaque supports (workstation, tablettes…) et achat puis configuration de badges personnalisés avec photo et puce (sans RFID car facilement clonable malgré l'aspect pratique) pour accéder aux locaux (voir le tableau suivant concernant la mise en place d'une barrière).
- Les habilitations seront en cohérence avec la politique de classification de l'information (allant de public à secret défense).

- Deny by default (« Tout est généralement interdit sauf autorisation expresse »), sauf pour le personnel autorisé selon les principes de besoin de connaître et d'utiliser justifiés par le besoin métier. Les droits seront revus périodiquement (tous les 3 mois)
- Accès qu'à l'information dont un utilisateur aurait besoin pour réaliser ses tâches. Par exemple le comptable habilité à consulter et modifier les données dans le logiciel de comptabilité EBP, n'aura pas accès aux données RH des autres employés.
- Indiquer dans la charte informatique voire le contrat de travail, une déclaration par laquelle ils s'engagent à ne pas divulguer leurs informations secrètes d'authentification personnelle volontairement ni involontairement (post-it avec mots de passe sur le moniteur, carte personnelle laissée sur le bureau…)
- Adapter les droits d'accès des utilisateurs qui ont changé de fonction ou de poste
- Accès qu'aux moyens de traitement de l'information (matériel informatique, applications, procédures, salles) dont un utilisateur aurait besoin pour accomplir sa tâche/son travail/son rôle. L'accès au bureau de la direction doit être limité au gérant de l'entreprise, un commercial n'a pas à y accéder.
- Etablir une procédure claire et précise en matière d'autorisation des requêtes d'accès (via un formulaire par exemple).
- Suppression ou blocage immédiats des identifiants et cartes d'accès aux locaux/ressources informatiques des employés qui ont quitté l'organisation.
- Préciser dans la charte informatique ou contrat de travail les sanctions encourues en cas de tentative d'accès non autorisé par un salarié ou un prestataire (SLA)
- Archivage des enregistrements de tous les événements significatifs relatifs à l'utilisation et des accès données/retirés.

Biens	Clause ISO 27001
• Matériels : (3 ordinateurs, 1 NAS, 1 HD externe, Firewall, Imprimante HP, 1 ordinateur portable + Dock, 2 tablettes numériques, 1 vidéoprojecteur, 5 smartphones android, Nas, bureaux, Hub, mini baie de brassage, téléphone fixe, volets roulants, parking…)	A.11.1.1
Catégorie de contrôle / Mesure	**Contrôle / Mesure**
Périmètre de sécurité physique	Il convient de définir des périmètres de sécurité servant à protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.
Contrôles physiques des accès	Il convient de protéger les zones sécurisées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.
Sécurisation des bureaux, des salles et des équipements	Il convient de concevoir et d'appliquer des mesures de sécurité physique aux bureaux, aux salles et aux équipements.
Protection contre les menaces extérieures et environnementales	Il convient de concevoir et d'appliquer des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents.

Emplacement et protection du matériel	Il convient de déterminer l'emplacement du matériel et de le protéger de manière à réduire les risques liés à des menaces et dangers environnementaux et les possibilités d'accès non autorisé.
Sécurité du câblage	Il convient de protéger les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information contre toute interception, interférence ou dommage.
Maintenance du matériel	Il convient d'entretenir le matériel correctement pour garantir sa disponibilité permanente et son intégrité.
Sortie des actifs	Il convient de ne pas sortir un matériel, des informations ou des logiciels des locaux de l'organisation sans autorisation préalable.
Sécurité du matériel et des actifs hors des locaux	Il convient d'appliquer des mesures de sécurité au matériel utilisé hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site.

Matériel utilisateur laissé sans surveillance	Il convient que les utilisateurs s'assurent que le matériel non surveillé est doté d'une protection appropriée.
Mise au rebut ou recyclage sécurisé(e) du matériel	Il convient de vérifier chacun des éléments du matériel contenant des supports de stockage pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut ou sa réutilisation.
Politique du bureau propre et de l'écran vide	Il convient d'adopter une politique du bureau propre pour les documents papier et les supports de stockage amovibles, et une politique de l'écran vide pour les moyens de traitement de l'information.

Mise en œuvre

- Identifier clairement les salariés et les tiers qui sont autorisés au retrait des actifs du site (smartphones pro, tablettes, appareils nomades) en fixant des limites dans le temps pour la sortie des actifs et de vérifier que la date de retour est respectée;
- Sensibiliser le personnel pour ne pas laisser le matériel et les supports de données sortis des locaux sans surveillance dans des lieux publics, sans oublier la discrétion (exemple : la tablette Android mise en évidence sur le tableau de bord de la voiture de fonction).
- Ajouter aux campagnes de sensibilisation sur la sécurité du SI, les mesures de protection du matériel laissé sans surveillance en interne (campagne annuelle avec des ateliers ou réunions).

- Verrouillage systématique des sessions (postes de travail et mobiles) en cas d'absence et mise en place d'un économiseur d'écran protégé par mot de passe. Déconnection après fin d'utilisation.
- Déplacer l'imprimante pour éviter qu'elle soit accessible au public (dans un des bureaux) et paramétrer un code pour pouvoir utiliser l'imprimante. Retirer immédiatement des imprimantes les documents contenant de l'information sensible ou classée.
- Discrétion externe : ne pas manifester à extérieur ou intérieur, des signes qui attiserait les convoitises. Par exemple, recourir à des décorations neutres, enlever les signes de richesse extérieurs. S'assurer que les informations confidentielles ne soient pas audibles de l'extérieur avec le double vitrage des fenêtres.
- Disposer le matériel nomade dans le bureau de la direction (avec armoire digicode) pour éviter que les commerciaux puissent entrer dans le local technique. Ce choix peut poser à débat mais c'est une possibilité. L'idée est de réduire l'accès physique au maximum aux biens à forte valeur business.
- Ne pas indiquer sur la porte, ni afficher qu'il s'agit du local technique. Seul le personnel habilité sera tenu au courant.
- Lors du recyclage et la destruction du matériel : s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant sa mise au rebut ou sa réutilisation. Chiffrer l'intégrité des disques durs et supports amovibles et de logiciel pour écraser les informations après chiffrage (Ashampoo HDD Control 3, qui permet aussi de monitorer et vérifier le bon état des disques durs). Cette mesure vient en complément du dégaussage et la destruction physique des appareils amovibles mais aussi les disques durs des appareils fixes.
- Achat d'un broyeur pour les documents papiers afin d'éviter la fouille dans les poubelles.
- Equiper l'ensemble du local d'un paratonnerre. On suppose que les lignes électriques et de télécommunication entrantes sont équipés de parafoudres vu la zone économique.
- Planifier en entretien annuel en vue de prévenir les fuites d'eau car le local technique est à côté des toilettes. Lors de cet entretien, vérifier que la VMC, climatisation restent efficaces autant dans le local

technique que le reste de l'entreprise. Vérifier régulièrement la température, le niveau d'humidité par l'administrateur/ responsable technique.

- Lorsque l'entreprise à recours à un dépannage informatique externe : mettre en œuvre des mesures appropriées lorsque la maintenance d'un matériel est réalisée par un personnel extérieur à l'entreprise (suppression des données temporaires pour le dépannage lors de la maintenance, non divulgation des données de l'entreprise). Après l'intervention, inspecter le matériel pour s'assurer qu'il n'a pas subi d'altérations et qu'il fonctionne correctement.
- Conserver un dossier de toutes les pannes suspectées ou avérées et de toutes les tâches de maintenance préventives ou correctives;
- Protéger le boitier électrique avec une clef et séparer les câbles électriques des câbles de télécommunication pour éviter toute interférence. Installer un blindage électromagnétique pour assurer la protection des câbles au niveau du local technique.
- Installer des cadenas/antivols sur le matériel informatique lorsque c'est possible en priorisant les biens en terme de valeur (les postes Workstation, le Nas, le serveur de données FTP…)
- Mise en place de portes blindés pour accéder au local technique et le bureau de la direction avec double authentification (digicode + carte d'identification).
- Surveillance de l'entrée principale avec caméra à rotation 360° qui permet également d'enregistrer les personnes qui rentrent dans le bureau de la direction et du local technique.
- Installation de 7 Détecteurs de fumée répartie par pièce, normé NF EN 14604
- ~~Eclairage du parking (en hauteur pour que le local de l'entreprise soit visible également la nuit)~~
- Détecteurs de mouvements à la porte d'entrée principale.
- Système d'alarme à niveau des fenêtres avec loquets de sécurité et de la porte d'entrée avec notification auprès du dirigeant.
- Mise en place d'un grillage/clôture sur la largeur du terrain côté rue avec portillon pour accéder à l'allée qui mène à la porte d'entrée du local.

- Indiquer dans charte d'utilisation, l'interdiction de fumer dans les locaux.
- Le parking est à découvert mais protéger contre les attaques béliers avec des poteaux à disposer sur la largeur du terrain. Pour l'emplacement du parking (on suppose qu'il y a 4 place), disposer des arceaux anti-stationnement.
- Revoir abonnement électricité pour la haute disponibilité, vérifier les conditions et garanties SLA pour le FAI+ achat 2 onduleurs (PCA électricité)
- **DISPOSER 2 EXINCTEURS DE CLASSE B (1 A L'ENTREE ET UN DANS LE HALL ENTRE LE LOCAL TECHNIQUE ET LE BUREAU DE LA DIRECTION) ET UN EXTINCTEUR DE TYPE B AVEC CO2 EN CAS DE FEU AU NIVEAU DES SERVEURS, EQUIPEMENTS ELECTRIQUES.**
- **EXTINCTEUR AUTOMATIQUE A EAU (SPRINKLER) SUR LES PLAFONDS NF EN 12845, APSAD R1 ?**
- Enregistrer à l'accueil du bâtiment les heures d'arrivée et de départ avec vérification par l'hôte/l'hôtesse d'accueil de véracité du rendez-vous.
- Surveillance particulière des personnes exceptionnellement présente sur le site et disposant d'une autorisation temporaire. Tenir un carnet de registre.

APRES LA MISE EN PLACE DES MESURES : RISQUE RESIDUEL (SELON LA METHODE EBIOS RM 2018)

Risque C : **Incendie dans la salle des serveurs**

■ Description sommaire : Mauvaise ventilation du NAS ou de la mini baie de brassage et détecteur de fumée absent

■ Vulnérabilités résiduelles susceptibles d'être exploitées par la source de risque : Panne des ventilateurs, accumulation de poussières

■ Autres causes ou facteurs aggravants (négligence, erreur, concours de circonstance, etc) : câbles non protégés qui peuvent créer un départ d'incendie, cigarette et autres combustibles

Événements redoutés concernés :

■ Événement redouté : Destruction du matériel et des données clients

Mesures de traitement du risque existantes et complémentaires :

■ Mesure : Achat de ventilateurs pour les serveurs, câblage correcte au niveau de la mini baie de brassage + entretien de la VMC

■ Mesure : Contrôle des applications qui utilisent trop de ressources systèmes et chauffent les composants

■ Mesure : Dispositif de détecteur de fumée dans la salle des serveurs conforme NF EN 14604

■ Mesure : Mise en place de sauvegardes supplémentaires sur site (hebdomadaire) sur des bandes magnétiques en plus du NAS + Hors site via Azure cloud (certifié PASSI et ISO 27017).

Evaluation du risque résiduel					
Gravité initiale	Critique	Vraisemblance initiale	Peu vraisemblable	Niveau de risque initial	
Gravité résiduelle	Grave	Vraisemblance résiduelle	Peu vraisemblable	Niveau de risque résiduel	

Gestion du risque résiduel : Contrôle annuel du détecteur de fumée et monitoring des ressources systèmes (CPU, GPU, Disques Dur avec alerte au-delà de 120°

Risque A : **Mise en place d'un keylogger et d'une backdoor**

■ Description sommaire : Accès physique au local technique non protégé et mot de passe des comptes faibles

■ Vulnérabilités résiduelles susceptibles d'être exploitées par la source de risque : Attaque par mouvements latéraux possible après élévation de privilèges, consulter les logs des outils de sécurité du SI en corrélation avec les SIEM.

■ Autres causes ou facteurs aggravants (négligence, erreur, concours de circonstance, etc.) : Tentative de phishing (dépôt de supports amovibles type clés usb sur le parking, supports amovibles offert par des faux jeux-concours ou quelqu'un de malveillant…)

Événements redoutés concernés :

■ Événement redouté : Cout important. Perte de confiance clients, défiance des actionnaires et des partenaires, risques pénales (violation RGPD…)

Mesures de traitement du risque existantes et complémentaires :

■ Mesure : Mise en place d'une porte blindée avec badge numérique + boitier d'authentification par mot de passe

■ Mesure : Mise en place du verrouillage automatique de compte avec économiseur d'écran + mot de passe

■ Mesure : Politique de mot de passe avec 8 caractères dont alphanumériques + spéciaux à changer chaque mois.

■ Mesure : Paramétrer l'anti-malware pour le scan des ports USB avant de pouvoir l'exécuter.

■ Mesure : Désactiver les réseaux sans fils non utilisés

Evaluation du risque résiduel					
Gravité initiale	Grave	Vraisemblance initiale	Très vraisemblable	Niveau de risque initial	

Gravité résiduelle	significative	Vraisemblance résiduelle	Peu vraisemblable	Niveau de risque résiduel	

Gestion du risque résiduel : Audit interne, tests de pénétration physique périodique, maintenance des outils de protection et d'identification.

Budget (prix public avec tarif moyen sans comparatif)

INVESTISSEMENTS	**Montant € avec TVA**
Immobilisations corporelles	**666**3.8
Antivol à clé 1.50 mètre X4	47.76
Armoire à clés haute sécurité x1	288.75
Lecteur de carte à puce x4	78.96
Carte à puce ISO 7816 (lot de 20)	19.89
Destructeur de document x1	25.99
Smartphone Professionnel Crosscall Core x 5	299.5
Abonnement téléphone pro Orange x5 sur 1 an	1020
Paratonerre x1	*2175*
Cables réseau blindés x3	*44.36*
Caméra x1	*97*
2 Portes blindés simple + pose avec digicode	*2800*
Grillage 10 mètres	*349.90*
Portillon x1	*339.90*
7 détecteurs de fumée	*111.3*
Système d'alarme bâtiment X1	*290.24*
Arceaux anti-stationnement x4	*352*
Onduleurs x2	*239.8*
Extincteurs x2	*219.8*
	-

Immobilisations incorporelles	**13**
Ashmpoo HDD control 3	13
Frais de personnel (fourchettes)	***3030***
Frais d'installation et de configuration (60 jours X 14 euros/H pour le responsable technique-administrateur)	*1120*
Frais d'installation matériel de protection interne/externe	*650*
Frais d'entretien	*220*
Campagne de sensibilisation initiale (1 journée, 5 personnes)	*520*
Campagne de sensibilisation annuelle (1 journée, 5 personnes)	*520*
TOTAL	**9706.8**

La plus grande difficulté ne se situe pas au niveau du budget mais dans l'acceptation du changement, la sensibilisation du personnel pour garantir la mise en place et le maintien de la sécurité du personnes, des données, du système d'information, du matériel.