D2 - Participer à la gestion des risques de la PME

Activité 2.5 – Participation à la gestion des risques non financiers de la PME

Chapitre 10 – La gestion des risques informatiques

Problématique

L'informatique est au cœur du système d'information de l'entreprise. La généralisation des réseaux facilite la communication, le travail collaboratif, la sauvegarde des données et améliore la productivité. Mais l'interconnexion des appareils fragilise également l'organisation car une altération du système informatique accidentel ou malveillant peut bloquer le fonctionnement d'un poste, d'un service ou de l'entreprise ou conduire à des vols de données.

Pour sécuriser son fonctionnement l'entreprise doit identifier les risques et leurs apporter des solutions adaptées afin de protéger le matériel, les logiciels et les données. Ces protections passent par la mise en place :

- d'un **antivirus** et d'un **pare-feu** performants et à jour ;
- de **sauvegardes** des données fiables et pérennes sur disque dur interne ou externe en Cloud ;
- une **formation** et une **sensibilisation** du personnel aux bonnes pratiques digitales.

L'entreprise doit également protéger les données personnelles de ses salariés et celles collectées auprès de ses abonnés ou clients en respectant les règles européennes de la RGPD et du Governance Act sous peine de sanctions.

Le recourt au cloud computing apporte souvent des solutions performantes dans la gestion des données et de leurs sauvegardes et une plus grande souplesse dans la gestion des logiciels qui sont en mode SaaS.

Sommaire (8 h 10')

Introduction

Chapitre 10 – La gestion des risques informatiques - QCM

Questions	Avant	Réponses	Après
Question 1 L'appareil qui relie les matériels d'un réseau est	☐	Un routeur	☐
	☐	Un commutateur	☐
	☐	Un serveur	☐
Question 2 L'appareil qui relie 2 réseaux est	☐	Un routeur	☐
	☐	Un commutateur	☐
	☐	Un serveur	☐
Question 3 Les matériels sont identifiés sur un réseau par	☐	Une adresse digitale	☐
	☐	Une adresse numérique	☐
	☐	Une adresse IP	☐
Question 4 Le logiciel qui paramètre un ordinateur ou un réseau est le	☐	Système d'exploitation	☐
	☐	Système d'application	☐
	☐	Système boots	☐
Question 5 Le serveur NAS est un serveur	☐	D'applications	☐
	☐	D'impression	☐
	☐	De messagerie	☐
	☐	De fichiers	☐
Question 6 L'onduleur	☐	Régule les ondes WiFi	☐
	☐	Maintien l'électricité en cas de coupure	☐
	☐	Relie les matériels par ondes radio	☐
Question 7 Le logiciel qui crypte les données d'un disque dur est	☐	Un virus	☐
	☐	Un Trojan	☐
	☐	Un Ransomware	☐
	☐	Un Spyware	☐
Question 8 La 1re chose à faire lorsqu'un logiciel rançonneur est détecté consiste à	☐	Eteindre l'ordinateur	☐
	☐	Prévenir le responsable informatique	☐
	☐	Retirer le câble réseau de l'ordinateur	☐
Question 9 Un Trojan est également appelé cheval de Troie	☐	vrai	☐
	☐	faux	☐
Question 10 Un pourriel est	☐	un courrier non sollicité	☐
	☐	un fichier contaminé	☐
	☐	un email contaminé	☐
Question 11 L'antivirus doit être mis à jour	☐	tous les jours	☐
	☐	toutes les semaines	☐
	☐	tous les mois	☐
Question 12 Un système biométrique permet de contrôler	☐	la taille des personnes	☐
	☐	l'accès des personnes	☐
	☐	la chaleur de l'ordinateur	☐
	☐	la vitesse de l'ordinateur	☐
Question 13 Un antivirus protège contre	☐	les négligences	☐
	☐	les hackers ou pirates	☐
	☐	les intrusions	☐
	☐	les virus	☐
Question 11 Un mot de passe fort doit respecter les règles suivantes	☐	Faire plus de 8 caractères	☐
	☐	Contenir des majuscules et des minuscules	☐
	☐	Être facile à mémoriser	☐
	☐	Contenir des caractères spéciaux	☐
Question 12 Les mesures Européennes destinées à protéger les informations personnelles sont dans	☐	La RPGD	☐
	☐	La PRGD	☐
	☐	La RGPD	☐
Question 13 La cloud computing consiste	☐	À externaliser les sauvegardes de données	☐
	☐	À utiliser des logiciels en lignes	☐
	☐	À relier les ordinateurs	☐

Réflexion 1 – Identifier l'origine de risques informatiques

Durée : 20'	 *ou*	**Source**

Travail à faire

Après avoir lu le document, répondez aux question suivantes :

1. Quelles sont les principales conséquences d'une cyberattaque ?
2. Pourquoi est-il important de former le personnel aux risques informatique ?
3. Pourquoi faut-il mettre à jour régulièrement les logiciels et les pilotes informatiques ?
4. Pourquoi l'entreprise doit-elle veiller à respecter la RGPD par exemple ?

Doc. Les risques informatiques et numériques

Les risques informatiques et numériques peuvent avoir un impact significatif sur les entreprises, tant sur le plan financier que sur le plan opérationnel. Il est donc important pour elles de mettre en place des mesures de sécurité pour se protéger. En mettant en place ces mesures, les entreprises peuvent réduire le risque de subir des dommages dus à des cyberattaques, des erreurs humaines, des pannes matérielles ou des changements technologiques.

Les principaux risques informatiques et numériques d'une entreprise sont les suivants :

- **Les cyberattaques** sont les menaces les plus graves pour les entreprises. Elles entraînent des pertes de données, des interruptions d'activité, des dommages à la réputation et des pertes financières.

  Elles peuvent prendre de nombreuses formes :
  - les **virus** qui altèrent des fichiers ou le fonctionnement des ordinateurs ;
  - les **ransomwares** qui cryptent les données et rendent le système informatique inutilisable tant qu'une ranson n(a pas été payée ;
  - les **attaques par déni de service (DDoS)** qui submergent les serveurs d'une entreprise et bloque ou perturbe les opérations ;
  - **l'espionnage industriel et les logiciels espion**s qui s'approprient des informations confidentielles, etc.
- **Les erreurs humaines** sont également une source importante de risques informatiques, notamment lorsque les salariés sont mal formés. Les employés peuvent commettre des erreurs suivantes :
  - la **perte ou la destruction de données** à l'occasion de travaux courant sur les fichiers ou bases de données ;
  - la **divulgation d'informations** sensibles tel que l'identifiant ou le mot de passe noté sur un post-it ;
  - la **configuration incorrecte** des systèmes informatiques qui n'ont pas fait l'objet d'une mise à jour régulières ;
  - **l'ouverture inappropriée d'un fichier** avec une pièce jointe contenant un virus ou un ransomware qui infecte et bloque le serveur. Le Phishing et Ingénierie Sociale sont souvent utilisés pour tromper les employés et obtenir un accès non autorisé.
- **Les pannes et problèmes matériels** peuvent également entraîner des pertes de données ou des interruptions d'activité. Elles peuvent être causées par des facteurs tels que
  - des **catastrophes naturelles**, des **accidents ou des défauts de fabrication** ;
  - les **retards de mises à jour de Sécurité** peuvent rendre les systèmes vulnérables aux nouvelles menaces. Elles concernent les antivirus, les pilotes matériels et logiciels et les logiciels eux même. Ces éléments peuvent contenir des failles logicielles qui sont exploitées par les hackeurs.
  - **Les changements technologiques** peuvent également présenter des risques. L'entreprises doit s'assurer que son système informatique est compatible avec les nouvelles technologies.
- **La non-conformité aux lois et réglementations** en matière de protection des données peut entraîner des sanctions pénales et financières et affecter la réputation de l'entreprise. C'est notamment le cas si l'entreprise ne respecte pas la RGPD.

Voici quelques mesures de sécurité que les entreprises peuvent mettre en place pour se protéger contre les risques informatiques et numériques :

- installer un logiciel antivirus et anti-malware ;
- former les employés aux bonnes pratiques de sécurité informatique ;
- mettre en place une politique de sécurité informatique ;
- effectuer des sauvegardes régulières des données ;
- gérer les accès aux systèmes informatiques ;
- surveiller les systèmes informatiques pour détecter les activités suspectes.

Réflexion 2 – Identifier les avantages et les risques liées aux réseaux

Durée : 20’	 *ou*	**Source**

Travail à faire

Après avoir lu les **documents 1**, répondez aux questions suivantes :

1. Quels sont les principaux avantages des réseaux informatiques ?
2. Quels sont les inconvénients des réseaux informatiques ?
3. Quels sont les effets d’un ransomware ?
4. Que faire lorsqu’il est détecté ?
5. Quelles sont les conséquences du ransomware pour la ville d’Annecy ?
6. Que s’est-il passé en 2023 à Annecy.

Doc. 1 Les bons et les mauvais côtés des réseaux informatiques

Source : www.eds.com

Un réseau informatique est essentiellement constitué de plusieurs machines et de matériels ayant besoin d’être reliés entre eux pour remplir leur fonction primaire. Il n’y a cependant pas que des avantages à s’en servir, mais aussi des inconvénients.

LES AVANTAGES DES RÉSEAUX INFORMATIQUES

Les avantages offerts par les réseaux informatiques sont multiples. Ils permettent de faire des partages de fichiers et y avoir accès même à distance. Procéder à l’enregistrement, mais aussi copier tous les fichiers qui peuvent être utiles, tout cela grâce à un périphérique spécialement conçu pour stocker des données. Il est tout aussi possible, pour qui le veut, de faire des mises à jour de tous ces fichiers emmagasinés.

POSSIBILITÉ DE PARTAGER LES RESSOURCES

Le partage des ressources est aussi un atout indéniable et permet à plusieurs personnes d’utiliser les mêmes ressources pour accéder à Internet simultanément s’ils le désirent. Un autre avantage, qui a son importance, c’est sa capacité à stocker une multitude de données. De plus, la création d’un serveur est également possible, afin de permettre un stockage plus conséquent. Une méthode très utilisée par les entreprises afin d’éviter les bugs.

LES MAUVAIS CÔTÉS DES RÉSEAUX INFORMATIQUES

Les principaux inconvénients des réseaux informatiques sont les soucis liés à la sécurité. Si un ordinateur est connecté sur un réseau, il serait plus vulnérable à toutes sortes d’attaques. Un professionnel en informatique est capable de déceler rapidement un mot de passe et obtenir tous les renseignements qu’il désire. Heureusement, Il existe des logiciels pour sécuriser un serveur pour qu’aucun vol de dossiers secrets ne soit commis. Un des plus grands ennemis d’un ordinateur est le virus informatique qui a le pouvoir de contaminer le réseau entier, c’est-à-dire tous les ordinateurs qui sont reliés l’un à l’autre. Les virus peuvent les affecter rapidement à cause de l’interconnexion de tous les postes de travail.

Doc. 2 Les ransomwares

Les ransomwares sont des applications malveillantes utilisées par les cybercriminels. Il s’installe sur un ordinateur par un clic sur un lien ou une pièce jointe d’un document reçu. Il **bloque l’accès au système ou chiffre les données** de l’ordinateur puis les données du réseau auquel l’ordinateur est connecté. Les cybercriminels demandent une rançon à leurs victimes en échange de leurs données. Lorsqu’un Ransomware est détecté, l’ordinateur doit être immédiatement débranché du réseau pour éviter qu’il ne se propage au réseau entier avant qu’il ne soit trop tard.

Doc. 3 Annecy fortement touchée par une cyberattaque

Source : le monde informatique ; Dominique Filippone, 26/11/2021

Frappée jeudi matin par une attaque informatique, la ville d'Annecy (Haute-Savoie) connait de très forts impacts sur ses services informatiques. Les démarches d'Etat civil reviennent au papier, la plupart des démarches en ligne sont impossibles et l'accueil téléphonique hors service.

François Astorg, le maire d'Annecy, a déposé plainte suite à la cyberattaque qui a frappé la ville ce jeudi 25 novembre 2021.

Quasiment un an après l'agglomération du grand Annecy, c'est cette fois au tour de la ville d'Annecy d'être touchée de plein fouet par une cyberattaque. Depuis jeudi matin, la collectivité connait de très séreuses indisponibilités de ses services et un plan de continuité de ses activités a été mis en place en urgence. Les démarches d'Etat civil sont désormais assurées par des formulaires au format papier (mariage, naissance, décès) et la plupart des services en lignes sont inopérants (portail service familles, prise de rendez-vous, bibliothèque municipale...). L'accueil téléphonique est touché également, remplacé par un numéro de mobile qui ne répondait pas à l'heure de l'écriture de cet article. Les inscriptions aux activités sportives municipales sont aussi impactées, mais pas le centre de vaccination dont les ordinateurs n'ont pas été touchés.

(Information complémentaire : en 2023 la mairie d’Annecy a été victime d’un nouveau Ransomware).

Réflexion 3 – Comprendre le rôle clé des sauvegardes informatiques

Durée : 20’	 *ou*	**Source**

Travail à faire

Après avoir lu le **document**, répondez aux questions suivantes :

1. Pourquoi la sauvegarde est un point clé de l'informatique ?
2. Quel avantage apporte une sauvegarde automatique ?
3. Quel est l'intérêt d'externaliser les sauvegardes ?
4. En quoi consiste la sauvegarde incrémentale et quel est son intérêt ?

Doc. Sauvegarde informatique d'entreprise, laquelle choisir ?

Source : www.itvisions.fr - 02-09-2020

La sauvegarde informatique permet de récupérer ses données à la suite d’une panne d’un disque dur, d’une mauvaise manipulation de suppression de données, de dégâts impactant les locaux de type incendie ou inondation, ou encore d’une perte de données résultant d’une attaque informatique. La sauvegarde informatique permet donc de mettre à l’abri les données de l’entreprise, et de les récupérer en cas de besoin. […]

Le fléau des nouvelles menaces informatiques : la sauvegarde informatique fait d’autant plus fait parler d’elle, qu’elle se trouve être l’ultime rempart dans le cas d’une attaque informatique par ransomware. […] Grâce à une sauvegarde efficace et fiable, les entreprises peuvent se libérer de ce type de menaces, sans avoir à payer la moindre rançon, et en conservant une parfaite intégrité de leurs données.

Nous présentons ci-dessous les différents types de sauvegardes possibles.

- **Sauvegarde informatique locale et Sauvegarde locale automatique**

- **La sauvegarde locale** correspond à une sauvegarde. Elle ne permet pas la récupération des données récentes, mais elle permet d’avoir un backup complet à un instant T sur un disque dur. L’entreprise doit mettre en place d’autres dispositifs en parallèle.
- **La sauvegarde locale automatique** assure d’une sauvegarde régulière des données dans un périphérique connecté au réseau local. Il peut s’agir d’un NAS (serveur de fichier) ou d’un simple disque dur externe. Les sauvegardes peuvent être journalières, hebdomadaires, mensuelles, etc.). Ce type de sauvegarde évite les oublis.

- **Sauvegarde externalisée physique**

Cette sauvegarde externalise la sauvegarde automatique sur une paire de disques durs, un par semaine par exemple. Chaque semaine un disque différent est remplacé pour être sorti des locaux et du réseau local. Ce roulement des sauvegardes externalisée est peu contraignant pour l’utilisateur mais nécessite une assiduité dans le changement des disques.

- **Sauvegarde Cloud simple**

Cette sauvegarde permet de stocker des données dans un espace alloué sur la plateforme d’un fournisseur. Les données deviennent ainsi accessibles depuis n’importe où grâce à une connexion internet. […] L’inconvénient de ce type de sauvegarde réside dans le fait que certains fournisseurs ne conservent pas les versions antérieures d’un fichier. La conséquence en est qu’un fichier corrompu ou modifié par erreur se retrouve aussitôt synchronisé et sauvegardé sur le cloud, sans possibilités de le restaurer. Certains acteurs du marché le proposent dorénavant.

- **Sauvegarde externalisée professionnelle**

Cette sauvegarde consiste à effectuer une copie des données vers des serveurs placés dans des Datacenters qui peuvent être répliqués. Ces Datacenters répondent à des exigences strictes en termes de disponibilité et de sécurité.

La **sauvegarde incrémentale** est la plus utilisée. Elle consiste à effectuer une première complète puis à n’enregistrer que les fichiers qui ont été ajoutés, modifiés ou supprimés ce qui réduire la taille et la durée des sauvegardes. Les sauvegardes sont effectuées de manière automatique et régulière. La sauvegarde hébergée conserve l’historique des versions de chaque fichier. Cette méthode permet une sauvegarde sûre et efficace des données avec une restauration facile des documents.

Attention cependant, la sauvegarde externalisée dépend de la connexion internet. Plus le lien internet, est puissant plus les sauvegardes sont rapides.

Dans l’idéal il est préférable de combiner une sauvegarde locale avec une sauvegarde externalisée pour se prémunir de tous les risques.

Réflexion 4 – Sensibiliser le personnel aux risques informatiques

Durée : 15’	 ou	**Source**

Travail à faire

À l'aide du **document** diffusé auprès des entreprises de Basse-Normandie, répondez aux questions suivantes,

- Quel est le rôle de ce document ?
- Quelles sont les caractéristiques des règles énoncées ?

Doc. Protégez votre information stratégique

Source : http://direccte.gouv.fr/IMG/pdf/passeport_protection_information.pdf

J’adapte ma conduite aux situations.

J’identifie

Au sein de l’entreprise, chacun possède une information stratégique : un savoir-faire ou une connaissance. Selon les niveaux, l’information est plus ou moins sensible. D’où la nécessité pour chaque acteur de l’entreprise de bien identifier son information stratégique, son noyau dur.
Il s’agit là d’identifier la menace qui pèse sur cette information.
La fuite de ce type d’information est très coûteuse pour l’entreprise et pour l’emploi.

Je protège au sein de l’entreprise

- Je fais « bureau net » ou je ferme mon bureau.
- Je gère les visiteurs et stagiaires : j’accompagne et je raccompagne mon visiteur. Je contrôle l’accès aux informations du stagiaire.
- Je respecte les règles de classification et de diffusion des documents papier (armoire, destruction…)
- Je surveille les opérations de maintenance.
- Je fais une utilisation prudente du téléphone, GSM, fax, visioconférence…
- Je porte mon badge.
- Je respecte les règles d’utilisation de la charte informatique (danger de certains sites, blog…).

Je protège à l’extérieur de l’entreprise

- **Au restaurant**, je [reste discret dans mes conversations], surtout près de mon lieu de travail.
- **À l’hôtel**, je ne me sépare pas de mes informations stratégiques.
- **Dans les salons**, je maîtrise l’information diffusée et je me méfie des faux clients !
- **En train ou en avion**, je suis prudent dans mes conversations et dans l’utilisation de mon PC portable.
- **En voyage**, je m’adapte aux us et coutumes locaux. Et surtout, je reste vigilant au téléphone, en déplacement, et sur ma vie privée.
- **Je prépare mes voyages à l’étranger**. J’expurge mon PC portable de toutes données sensibles et inutiles à mon déplacement. Je me munis des numéros de téléphones (ambassade) utiles sur place.

J’assure la sécurité des systèmes d’information

- Je respecte la charte informatique de mon entreprise. Tout ce qui traite, stocke et transmet de l’information est vulnérable.
- J’ai conscience que ma responsabilité et celle de l’entreprise peuvent être engagées en cas de non-respect de l’utilisation de l’outil informatique.
- Je protège mon PC portable contre le vol, la destruction ou les virus.
- Je maîtrise l’information que je délivre sur les réseaux sociaux, je ne parle pas de mon activité ou de mon entreprise car je communique des informations à la concurrence.

J’alerte

Je signale à ma direction toute :

- disparition d’objets ou de documents ;
- approche suspecte y compris dans ma vie privée ;
- personne inconnue circulant dans les locaux sans badge

Réflexion 5 – Choisir un mot de passe		
Durée : 10’	 *ou*	**Source**

Travail à faire

Voici une liste de mots de passe, donnez votre avis pour chacun d’eux.

Salariés	Mot de passe	Explication	Votre avis
Julien Goubert	**Julien**	Prénom	
Pauline Lecoeur	**28011976**	Date naissance	
Julie Pinel	**JUPI**	Code prénom + nom	
Paul Roncourt	**Louise-Elise**	Prénoms des enfants	
Etienne Buis	**LMELLDTE**	La Maladresse Est La Loi De Tout Essai	
Hervé Farge	**GRENOBLE78**	Lieu + année nais-sance	
Pierre Kerval	**G3E1FE2G**	J’ai trois enfants une fille et deux garçons	

Réflexion 6 – Identifier les risques encourus pour non respect des obligations légales

Durée : 15’	 *ou*	**Source**

Travail à faire

À l'aide des **documents 1 et 2**, répondez aux questions suivantes :

1. Quelle est la source de la RGPD ?
2. Quelle est sa finalité ?
3. Quels sont les risques pour l'entreprise en cas de non-respect de la RGPD ?
4. Quel est le risque encouru pour défaut de sécurité des informations nominatives ?

Doc. 1 Nouveau règlement européen : objectifs principaux et sanctions

Source : https://donnees-rgpd.fr/

Quels sont les objectifs du règlement européen ?

Ce texte comporte trois objectifs principaux, le principal étant la préservation des droits de chacun sur ses données personnelles.

Le nouveau règlement vise également à homogénéiser la législation et la réglementation au sein des 28 pays de l’Union européenne. Le RGPD sera d’application direct au sein de chaque pays membre.

En outre, la loi entend responsabiliser chaque individu en ce qui concerne le traitement des données sensibles.

L’Union Européenne entend bien faire respecter ces objectifs par le biais de **sanctions plutôt dissuasives**.

- **Les sanctions en cas d’infraction**

En effet, le nouveau règlement européen prévoit d’importantes amendes administratives envers les responsables de traitement et les sous-traitants en cas de manquement à leurs obligations.

Les autorités « chef de file » telle que la CNIL pourront tout d’abord prononcer un avertissement à l’entreprise retardataire. Si ce rappel à l’ordre ne suffit pas, l‘entreprise sera alors mise en demeure.

Le traitement des données personnelles pourra être également limité ou bien totalement interrompu. Les autorités auront également le pouvoir de rectifier ou d’effacer les données en question.

Le montant de l’amende administrative varie en fonction de différents paramètres (nature, gravité de la fraude…). et pourra atteindre les 20 000 000 euros, ou dans le cas d’une multinationale, 4% de son chiffre d’affaires mondial total du dernier exercice.

Enfin, de telles sanctions entraîneraient des conséquences désastreuses sur la réputation de l’entreprise qui risquerait de perdre à la fois son image de marque et ses clients.

- **En conclusion**

[…]

Pour rappel, ce nouveau texte inclut entre autres obligations la tenue d’un registre, la désignation d’un DPO* et la sécurisation des données sensibles.

*** DPO = Délégué à la protection des données**

Doc. 2 Article 226.17 du code pénal

…le fait de procéder ou de faire procéder à un traitement automatisé d'informations nominatives **sans prendre toutes les précautions utiles pour préserver la sécurité de ces informations et notamment empêcher qu'elles ne soient déformées, endommagées ou communiquées à des tiers non autorisés est puni de cinq ans d'emprisonnement et de 300.000 euros d'amende**

Ces sanctions s'appliquent au Directeur de l'organisme en qualité de représentant de la personne morale à charge pour lui de se retourner contre le ou les auteurs de l'infraction.

Réflexion 7 – Identifier les avantages et les inconvénients du Cloud computing

Durée : 20’	 *ou*	**Source**

Travail à faire

À l'aide du **document**, répondez aux questions suivantes :
1. Le cloud apporte-t-il un avantage financier ?
2. Que signifie une grande flexibilité ?
3. Quels sont les principaux avantages du Cloud pour l’entreprise ?
4. Quelles sont les limites du Cloud pour l’entreprise ?

Doc. Avantages et les inconvénients du cloud computing pour l’entreprise

L’entreprise qui a recourt au Clous computing délocalise une grande partie de ses services auparavant hébergés sur ses propres ordinateurs et infrastructures. Ils sont désormais sur le cloud (ou le nuage), qui est un ensemble de serveurs distants interconnectés. Les utilisateurs accèdent aux informations et services via une connexion internet ou un réseau privé. Les leaders sur le marché sont Microsoft Azure, Amazon Web Services, Google Cloud Platform, IBM et Salesforce.

- **La maîtrise du budget et la réduction des coûts**

Grâce au cloud, l’entreprise paie, par abonnement, uniquement pour les ressources, infrastructures et services nécessaires. Elle n’a plus à investir dans du matériel onéreux et de nouveaux logiciels. La répartition des investissements est faite dans le temps et garantit une maîtrise totale des dépenses. De plus, il n’y a plus à se souciez du renouvellement des équipements, ni du fonctionnement et de la maintenance des datacenters.

- **Une grande flexibilité et agilité**

Les besoins de l’entreprise sont évolutifs. Les solutions cloud s’y adaptent en temps réel. Il est possible d’allouer rapidement davantage de ressources ou d’options aux outils. L’entreprise est plus réactive et plus performante.

- **Une accessibilité optimisée**

Le cloud computing permet de ne plus dépendre d’un lieu géographique, ni d’un matériel ou d’un système d’exploitation. Les collaborateurs bénéficient de tous les avantages d’une mobilité absolue depuis un simple navigateur web sur tous les supports connectés à internet existants (ordinateur, mobile, tablette…) ; les données sont entièrement centralisées et disponibles 24 h sur 24 et 7 j sur 7.

- **Un support idéal pour le travail en mode collaboratif**

Grâce au cloud, les collaborateurs sont reliés entre eux via une plateforme centralisant l’ensemble des canaux utilisés. Ils communiquent mieux et partagent leurs fichiers et leurs commentaires de n’importe où. Les mises à jour des documents sont faites en temps réel.

- **Une innovation en continu**

Les fournisseurs de services cloud mettent régulièrement à jour leurs offres. Ils garantissent de profiter des toutes dernières technologies sur l’ensemble des outils et applications.

- **Un engagement pour l’environnement**

Le cloud réduit la consommation électrique en favorisant la mutualisation des ressources sur de mêmes serveurs.

- **La sécurité des données garanties par le fournisseur**

- Le cloud computing apporte des garanties de sécurité supplémentaires. Le stockage et la sauvegarde des données sont fait sur un serveur externe et les services fonctionnent sur ce dernier. L’entreprise n’a plus à craindre les défaillances matérielles.
- La confidentialité et la protection de des données sont assurées par des dispositifs et services performants (chiffrement des datas, sécurisation des datacenters, etc.). En outre, choisir un serveur localisé en Europe permet de bénéficier de la législation européenne sur la RGPD.

- **Quelques inconvénients du cloud computing**

Le système du cloud computing révèle quelques inconvénients :
- Les réseaux informatiques restent attaquables et les services virtuels peut être mis hors fonction.
- L’entreprise dépend d’un prestataire externe. Il doit offrir des garanties solides et connaître les besoins de l’entreprise.
- Les services nécessaires à l’activité dépendent de la connexion internet. Une panne peut perturber l’organisation.
- L’entreprise perd une partie de la maîtrise de son système informatique.

Réflexion 8 – Comprendre le Governance Act et le Data Act

Durée : 20’	 *ou*	**Source**

Travail à faire

À l'aide du **document**, répondez aux questions suivantes :

1. Quelle est la finalité du *Data Governance Act* ?
2. Quelle est la finalité du *Data Act* ?
3. Quels sont les résultats attendus ?

Doc. 1 Le Data Governance Act (DGA) et le Data Act

Le Data Governance Act (DGA) et le Data Act sont deux textes législatifs européens qui visent à développer un marché unique de la donnée en Europe. Ils ont été adoptés en 2022 et 2023 respectivement, et sont entrés en vigueur le 24 septembre 2023.

Le Data Governance Act

Le Data Governance Act vise à faciliter la réutilisation des données publiques et détenues par des organismes privés. Il définit un cadre réglementaire pour les intermédiaires de données, qui sont des acteurs qui facilitent la mise en relation des personnes qui disposent de données avec celles qui souhaitent les réutiliser.

Le DGA prévoit notamment les mesures suivantes :

- La création d'un registre européen des intermédiaires de données, afin de garantir leur transparence et leur fiabilité.
- L'obligation pour les intermédiaires de données de respecter les droits des personnes concernées par les données, notamment le droit à la protection des données personnelles.
- L'établissement d'un cadre juridique pour la réutilisation des données publiques, afin de la rendre plus facile et plus transparente.

Le Data Act

Le Data Act vise à favoriser l'utilisation des données industrielles. Il définit un cadre réglementaire pour le partage et la réutilisation des données par les entreprises, notamment les données produites par les machines et les objets connectés.

Le Data Act prévoit notamment les mesures suivantes :

- Le droit pour les entreprises de demander à leurs fournisseurs de données de leur fournir des données dans un format ouvert et lisible par machine.
- Le droit pour les entreprises de réutiliser les données qu'elles ont collectées auprès de leurs clients ou de leurs partenaires commerciaux, sous réserve du respect des droits des personnes concernées.
- L'obligation pour les entreprises de prendre des mesures pour garantir la sécurité et la confidentialité des données qu'elles partagent ou réutilisent.

Ensemble, le DGA et le Data Act constituent un cadre réglementaire ambitieux pour le développement du marché unique de la donnée en Europe. Ces textes devraient permettre de faciliter l'accès aux données, de favoriser l'innovation et de stimuler la croissance économique.

Impacts attendus

Les deux textes sont susceptibles d'avoir un impact significatif sur le marché de la donnée en Europe. Ils devraient notamment permettre :

- De faciliter le partage et la réutilisation des données, ce qui pourrait contribuer à l'émergence de nouveaux produits et services innovants.
- De stimuler la concurrence, en favorisant l'accès des entreprises à des données plus diversifiées.
- De créer de nouveaux emplois, dans le secteur des données et de l'intelligence artificielle.

Cependant, il est encore trop tôt pour évaluer l'impact réel de ces textes. Leur mise en œuvre effective nécessitera la collaboration des États membres et des acteurs économiques.

Missions professionnelles

Mission 1 – Solutionner les problèmes de réseau et sensibiliser le personnel aux rançongiciels		Berod Recyclage
Durée : 1 h	*ou*	Source

Contexte professionnel

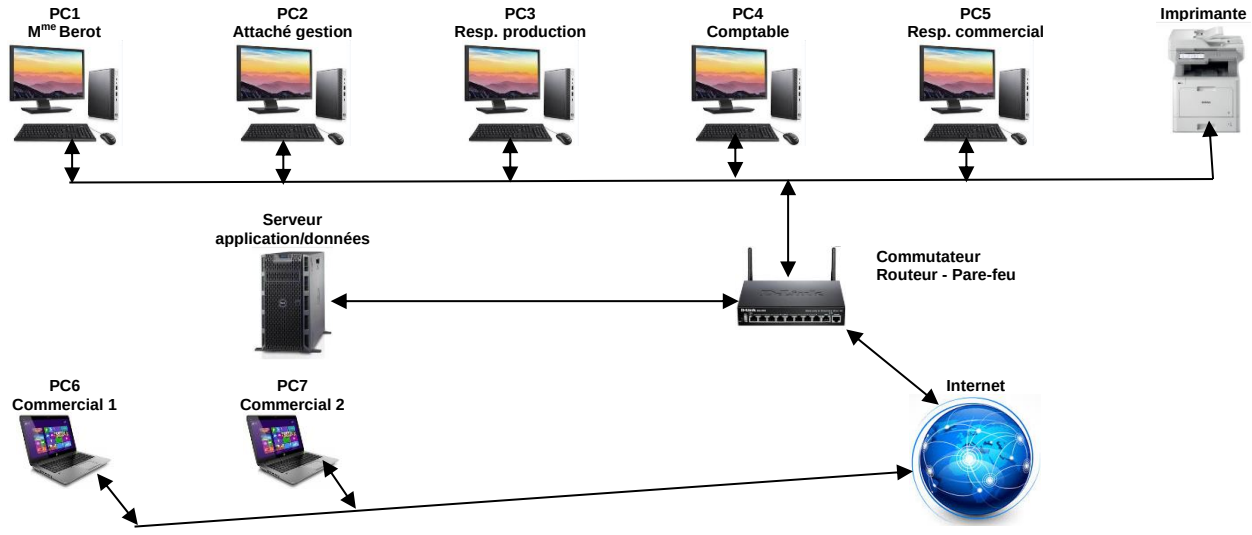
La société Berod a été créée par Sylvie Berod qui en est PDG. Elle est un référent métier dans la collecte et la gestion des déchets. Elle propose une solution globale dans le domaine du recyclage qui s'étend de la récupération des ferrailles et métaux au tri et à la valorisation des déchets. Elle travaille essentiellement avec les entreprises, les collectivités locales et les particuliers.

Dans le cadre de son activité quotidienne plusieurs **incidents** vous sont soumis. Vous devez en identifier les causes.

Travail à faire

1. À partir du **documents 1**, identifiez des causes possibles des incidents évoqués dans le **document 2** et proposez des actions adaptées aux situations en complétant le **document 2** (le nombre de ligne affichée en face de la panne indique le nombre de causes à trouver).
2. M^me^ Berod souhaite sensibiliser le personnel aux attaques par rançongiciel (ou ransomware). À l'aide des informations transmises dans **le document 3** créez une fiche d'explication sur l'attitude à avoir pour prévenir les attaques par rançongiciel.

Doc. 1 Schéma de l'organisation informatique de la société



Doc. 2 Problèmes rencontrés

Incidents rencontrés	Causes possibles	Solutions proposées
Aucun ordinateur du réseau ne parvient à se connecter à Internet		
Le PC2 ne parvient pas à se connecter à Internet alors que les autres ordinateurs y arrivent.		
Aucun ordinateur ne parvient à imprimer		
Le responsable de production ne peut plus accéder aux données commerciales du PGI		
Le PC 5 n'arrivent pas à imprimer alors que les autres ordinateurs y arrivent		
Internet fonctionne mais aucun ordinateur n'accède aux données des applications de gestion du réseau		
Lorsque l'ordinateur est allumé les noms des fichiers sont remplacés par code de type *1111111-AB11-4-DFG-FA12-038F3-2FE82D5.thor*		

Doc 3 Qu'est qu'un ransomware ou rançongiciel ?

Vous êtes de plus en plus nombreux à recevoir des messages douteux contenant des pièces jointes ou des liens vous invitant à les ouvrir.

Prenez garde ! Des logiciels malveillants appelés « rançongiciels » ou « ransomware » peuvent s'y cacher.

Leur but ? Chiffrer (coder) vos données pour vous les rendre moyennant une rançon. Bien entendu, la payer ne garantit pas la récupération de vos données. Mieux vaut donc vous prémunir contre ce type d'attaque.

Comment se prémunir d'un ransomware ?

- **Conseil n°1 : effectuez des sauvegardes régulières de vos données**

C'est le meilleur moyen de couper l'herbe sous le pied aux pirates souhaitant prendre vos données en otage ! Déplacez physiquement la sauvegarde de votre réseau (hors réseau), placez-la en lieu sûr et veillez à ce qu'elle fonctionne !

- **Conseil n°2 : n'ouvrez pas les messages dont la provenance ou la forme est douteuse**

Ne vous laissez pas tromper par un simple logo ! Pire, le hacker peut avoir récupéré certaines de vos données préalablement (les noms de vos clients par exemple) et créer des adresses de messagerie ressemblant à un détail près à celle de vos interlocuteurs habituels.

Restez donc très vigilants ! Certains messages paraissent tout à fait authentiques.

Apprenez à identifier les courriels piégés (ou autres formes de récupération de vos données) sur le site de l'**Agence nationale de la sécurité des systèmes d'information (ANSSI)**.

Vous avez un doute ? Contactez le messager par un autre biais.

- **Conseil n°3 : apprenez à identifier les extensions douteuses des fichiers**

Vous recevez habituellement des fichiers en .doc ou .mp4 (par exemple) et le fichier du message dont vous avez un doute se finit par un autre type d'extension ?

Ne les ouvrez surtout pas ! Voici quelques exemples d'extensions douteuses : .pif, .com, .bat ; .exe, .vbs, .lnk, ...

Attention à l'ouverture de pièces jointes de type .scr ou .cab. Comme le rappelle l'**Agence nationale de la sécurité des systèmes d'information (ANSSI)**, il s'agit des extensions de compression des campagnes CTB-Locker sévissant chez les particuliers, les PME ou les mairies.

- **Conseil n° 4 : mettez à jour vos principaux outils**

On ne vous le dira jamais assez : traitement de texte, lecteur PDF, navigateur mais aussi antivirus… Veillez à mettre à jour vos logiciels !

Si possible, désactivez les macros des solutions de bureautique qui permettent d'effectuer des tâches de manière automatisée. Cette règle évitera en effet la propagation des rançongiciels via les vulnérabilités des applications.

Considérez que, d'une manière générale, les systèmes d'exploitation en fin de vie, qui ne sont plus mis à jour, donnent aux attaquants un moyen d'accès plus facile à vos systèmes.

- **Conseil n° 5 : utilisez un compte « utilisateur » plutôt qu'un compte « administrateur »**

Évitez de naviguer depuis un compte administrateur. L'administrateur d'un ordinateur dispose d'un certain nombre de privilèges sur celui-ci, comme réaliser certaines actions ou accéder à certains fichiers cachés de votre ordinateur.

Préférez l'utilisation d'un compte utilisateur. Cela ralentira, voire dissuadera le voleur dans ses actions malveillantes.

Mission 2 – Gérer les comptes et les droits d'accès		Erbioline
Durée : 1 h	ou	Source

Contexte professionnel

La société ***Erbioline*** a été créée par **Camille Berthod** qui en est PDG. Elle conçoit des parfums, déclinés en crèmes et savons qu'elle fait fabriquer à Grasse, (Var), pour les parfums et à Venise pour les crèmes et savons. Elle reçoit les produits transformés et assure l'empaquetage et le packaging. Son activité est donc la suivante : achats ventes de parfums, savons, crèmes, achats ventes d'accessoires : rouges à lèvres, brosses…, création de parfums personnalisés, création d'ambiance olfactive pour l'évènementiel.

L'entreprise est équipée d'un réseau informatique et le responsable réseau souhaite le sécuriser par la création de groupe de travail dont les droits d'accès seront contrôlés. Dans ce contexte il vous est demandé de paramétrer les autorisations et les limitations d'accès aux espaces, fichiers, programmes. Ces droits seront paramétrés au niveau des groupes de travail.

Travail à faire

1. Définissez les groupes de travail dans le **document 1** (un groupe de travail regroupe des personnes dont l'activité est commune).

2. Définissez les autorisations d'accès aux dossiers dans le **document 2**. Le disque dur du serveur est accessible à tous. Mais M^me^ Berthod souhaite que les accès aux différents dossiers soient contrôlés. Indiquez pour chaque personne et dans chaque cellule les autorisations à paramétrer.

3. Définissez les autorisations d'accès aux programmes dans le **document 3**. Toutes les applications sont accessibles à partir du serveur. Paramétrez les autorisations d'utilisations des applications.

4. Définissez les autorisations d'accès à certains fichiers stratégiques dans le **document 4**. Tous les fichiers enregistrés dans l'espace commune sont accessibles à tous. Il vous est demandé dans les cas suivants d'indiquer les autorisations d'accès à paramétrer.

Doc. 1 Tableau du personnel

Placez une croix dans la colonne du groupe auquel une personne doit appartenir.
(*Remarque : le livreur reçoit ses ordres du responsable commercial et le technicien d'entretien du responsable de production. L'assistante de gestion travaille exclusivement pour la direction et le directeur administratif).*

Salariés	Groupe Direction	Groupe administratif comptable et financier DAF	Groupe Commercial	Groupe Production	Groupe Bureau étude
M^me^ Berthod PDG					
Comptable					
Commerciaux					
Responsable R et D					
Ingénieurs cosmétiques					
Responsable production					
Adjoint production					
Attachée de gestion					
Techniciens production					
Livreur					
Technicien d'entretien					

Doc. 2 Autorisation d'accès aux dossiers de travail

Les options suivantes sont possibles : ***Création (C) ; Interrogation (I) ; Modification (M) ; Suppression (S)***

Arborescence disque C: Serveur	PDG	Resp. informatique	Comp-table	Commer-ciaux	Produc-tion	Bu-reau étude
Système (OS)						
Programmes (applications)						
Périphériques (imprimante, scanneur, etc.)						
Données (espace de travail)						
Comptabilité						
Commercial						
Production						
Paie						
Recherche						
Espace travail commun						

Doc. 3 Autorisation d'accès aux programmes

(indiquez ***Oui*** *ou* ***Non****)*

Applications	PDG	Resp. informatique	Comptable	Commerciaux	Production	Bureau d'étude
Administration serveur						
Word						
Excel						
Access						
Powerpoint						
PGI Ventes - clients						
PGI Achats - fournisseurs						
PGI salariés - paie						
PGI production						
Outlook						
Jeux						

Doc. 4 Autorisation d'accès aux fichiers

Indiquez pour chaque groupe les fichiers auxquels ils peuvent avoir accès (indiquez **Oui** ou **Non**).

Fichiers	Direction	Administrateur	Commercial	Comptable	Production	Bureau d'étude
Base clients.dbf						
Suivi des clients.xlsx						
Statistiques commerciales.xlsx						
Base fournisseurs.dbf						
Statistiques des achats.xlsx						
Base salariés.dbf						
Bulletin de salaires.xlsx						
Suivi des arrêts.xlsx						
Courrier client.docx						

Mission 3 – Gérer des fichiers de données personnelles

Durée : 50’	ou	Source

Contexte professionnel

Alpes-Drones est spécialisée dans la commercialisation, l’adaptation et la maintenance de drones professionnels. Elle achète des drones puis les adaptes aux demandes des entreprises ou des particuliers par l’ajout de dispositifs techniques et d’applications dédiés à des tâches spécifiques à certains métiers : recherche de personnes ; sécurisation des pistes ; surveillance des lignes électriques et des barrages ; cartographie, etc.

Le directeur souhaite informatiser les informations commerciales et les informations clients.

Travail à faire

1. Créer une table Excel qui récapitule le détail des ventes réalisées et une table qui enegistre les informations clients. Réalisez ce travail à partir des factures qui vous sont remises dans le **document 1**.
2. Mettez à jour les tables créées.
3. Il s’interroge sur les obligations juridiques concernant la protection des données personnelles saisies dans des bases informatisées. Expliquez les contraintes liées à ce type de gestion de données en vous aidant des **documents 2** et **3**.

Doc. 1 Factures

Alpes-Drones
69 routes des Molettes, 38000 Grenoble.
Tél. : 04 78 54 23 30 **Site :** www.atd.com – info@atd.com.
SA au capital de 200 000 €.
SIRET : 463 550 565 54145. - **APE/NAF :** 8325 N.

Date Facture: **15 mai F45-71**

Dubreuil Emile
562 Ruel Merlios
38000 Grenoble

Réf.	Designaion	PU HT	Qté	Total
BUDJ4	Bundle DJI Mini 4	940,00	2	1 880,00
			Net HT	1 880,00
			TVA 20 %	376,00
			Net TTC	**2 256,00**

Alpes-Drones
69 routes des Molettes, 38000 Grenoble.
Tél. : 04 78 54 23 30 **Site :** www.atd.com – info@atd.com.
SA au capital de 200 000 €.
SIRET : 463 550 565 54145. - **APE/NAF :** 8325 N.

Date Facture: **18 mai F45-72**

Sorlier Louise
78 Rue des Astres
73000 Chambéry

Réf.	Designaion	PU HT	Qté	Total
HOVAIRX1	HoverAir X1	430,00	1	430,00
			Net HT	430,00
			TVA 20 %	86,00
			Net TTC	**516,00**

Alpes-Drones
69 routes des Molettes, 38000 Grenoble.
Tél. : 04 78 54 23 30 **Site :** www.atd.com – info@atd.com.
SA au capital de 200 000 €.
SIRET : 463 550 565 54145. - **APE/NAF :** 8325 N.

Date Facture: **22 mai F45-73**

ATMS
98 rue L. Terray
74400 Chamonix

Réf.	Designaion	PU HT	Qté	Total
BETFPV	Moteur BETAFPV	49,20	2	94,40
REPAR	MO réparation	70,00	1	70,00
TEST	MO test	70,00	0,5	35,00
			Net HT	199,40
			TVA 20 %	39,88
			Net TTC	**239,28**

Alpes-Drones
69 routes des Molettes, 38000 Grenoble.
Tél. : 04 78 54 23 30 **Site :** www.atd.com – info@atd.com.
SA au capital de 200 000 €.
SIRET : 463 550 565 54145. - **APE/NAF :** 8325 N.

Date Facture: **25 mai F45-74**

Germain Brugier
34 route des Fins
69000 Lyon

Réf.	Designaion	PU HT	Qté	Total
BRUSHF415	Moteur Brushless F415	72,00	2	144,00
REPAR	MO réparation	70,00	1,5	105,00
TEST	MO test	70,00	1	70,00
			Net HT	319,00
			TVA 20 %	63,80
			Net TTC	**382,80**

Doc. 2 Fichier clients : quelles sont les règles à respecter ?

Source : www.lemagdelentreprise.com

Un fichier client est un document précieux et indispensable pour une entreprise. Il compose une partie de sa valeur et contribue à son développement. Ce fichier contient toutes les coordonnées de ses prospects et de ses clients et permet d'accéder facilement aux renseignements qui permettent de les joindre rapidement. Un fichier client contient également toute l'historique des relations commerciales ainsi que celles qu'il convient de réaliser. Son analyse permet aussi à une entreprise de connaître exactement les comportements de ses clients et d'agir commercialement en fonction. Cet élément indispensable doit cependant respecter certaines règles et obligations concernant sa forme. Explications.

Que contient un fichier client ?

En général, un fichier client contient toutes les coordonnées personnelles des clients et prospects d'une entreprise. C'est-à-dire leur nom et prénom, leur adresse, leur date de naissance, leur téléphone et adresse e-mail, et éventuellement leur site internet.

Un fichier client va plus loin en rassemblant aussi des informations concernant les dates auxquelles des contacts ont été pris avec les clients et les prospects, l'historique des commandes passées, le chiffre d'affaires réalisé avec chacun d'eux et les actions commerciales futures à envisager.

Pour être efficace, un fichier client doit être mis à jour le plus régulièrement possible.

Quelles sont les obligations légales en matière de fichier client ?

En raison des données personnelles qu'il contient, un fichier client doit se conformer à des règles et des obligations légales, et notamment respecter le Règlement européen sur la protection des données (RGPD) en vigueur depuis le 25 mai 2018. Cette réglementation concerne toutes les informations à caractère personnel (nom, prénom, adresse électronique, localisation, numéro de carte d'identité, adresse IP, photo, profil social, etc.) détenues et conservées numériquement ou sur papier par les administrations, les collectivités, les associations, mais aussi les entreprises (quelle que soit leur taille).

Le RGPD peut sembler un outil compliqué et difficile à mettre en place pour les petites entreprises, mais comme le souligne la Commission nationale de l'informatique et des libertés (Cnil) : « Pas supplémentaire vers la digitalisation, cette nouvelle réglementation constitue également un levier d'amélioration de la gestion de l'entreprise et son efficacité commerciale ». Afin d'aider les petites structures à mettre en place le RGPD, la Cnil et Bpifrance, partenaire des entreprises, ont édité un guide qui tente de dédramatiser la mise en œuvre de cette règlementation qui touche également les fichiers clients.

D'autre part, hormis pour les entreprises du domaine bancaire, de l'assurance, de la santé et de l'éducation, chaque fichier client doit faire l'objet d'une déclaration auprès de la Cnil selon la norme simplifiée n° NS-048.

L'obligation d'information et d'accord des personnes présentes dans un fichier client

Le RGPD a pour premier objectif de faire respecter le droit des personnes. En conséquence, les données personnelles détenues dans un fichier client doivent répondre à une « utilisation loyale et transparente, explicite, pertinente et limitée aux finalités du traitement ». La réglementation stipule aussi que ces informations doivent être tenues à jour et conservées de manière temporaire et sécurisée. Dans une entreprise, l'accès aux données contenues dans un fichier client doit être limité aux personnes qui ont été désignées pour gérer ce support d'informations ou à des tiers qui y ont été autorisés.

Une entreprise qui détient un fichier client doit obligatoirement en informer les personnes qui y figurent et recueillir leur accord. Elle doit aviser ses clients et prospects concernés, d'une part qu'un tel fichier existe, et, d'autre part, l'entreprise doit fournir l'identité du responsable du fichier client, justifier de la finalité des renseignements détenus et à qui ils peuvent être transmis, et informer des droits d'accès, de rectification ou d'opposition.

À noter que toutes les entreprises de plus de 250 salariés doivent tenir un registre relatant toutes les activités de traitement réalisées sur leur fichier client.

Comment constituer un fichier client en respectant les règles ?

Une entreprise qui prospecte de nouveaux clients doit respecter certaines règles pour utiliser leurs coordonnées à des fins commerciales. Il convient par exemple de ne pas reprendre les informations accessibles gratuitement sur

Internet (sur un annuaire par exemple) sans prendre un minimum de précautions. Il peut s'agir en effet de personnes inscrites sur des listes spécifiques antidémarchage et donc qui ne sont pas d'accord pour être prospectées.

De la même manière, une entreprise doit se méfier des ventes à bas prix de fichiers de données personnelles en vente sur le net. Le plus souvent, il s'agit de données qui n'ont pas été collectées dans des conditions qui respectent les règles et obligations en vigueur.

Les prospects dont les données sont collectées doivent avoir donné leur accord au préalable (ce que l'on appelle le opt-in) ou ne pas avoir exprimé leur refus (le opt-out). Dans tous les cas, ils doivent pouvoir faire part de leur désaccord pour ne pas recevoir d'autres sollicitations commerciales à l'avenir.

Pour un fichier client déjà existant, les règles sont les mêmes que pour les prospects en matière de consentement. Pour se prémunir d'éventuelles plaintes auprès de la Cnil, une entreprise a tout intérêt à fournir un moyen simple à ses clients pour qu'ils puissent exercer leurs droits d'accès, de rectification, d'opposition et même d'effacement, le plus facilement possible. L'image et le sérieux de la société en dépendent.

Doc 3 Comment créer un fichier

Voici les 5 étapes à respecter pour créer un fichier clients conforme à la RGPD.

1. Définir les besoins

Définir les besoins de l'entreprise en matière de collecte et de gestion des fichiers clients. Cela passe par l'identification des données personnelles collectées, de leur finalité et des destinataires des données.

Le plus souvent les données personnelles collectées sont les suivantes : nom, prénom ; adresse postale ; e-mail ; téléphone ; date de naissance ; informations sur les achats effectués.

Ces données sont ensuite utilisées afin d'informer les clients sur les produits, les promotions et les événements ; pour des envois de newsletters ; et pour des actions marketing ciblées.

2. Élaborer une politique de confidentialité

Élaborer une politique de confidentialité qui précise les modalités de collecte et de traitement des données personnelles des clients. Cette politique doit être accessible aux clients et doit être rédigée de manière claire et concise.

La politique de confidentialité doit notamment mentionner les points suivants : les données personnelles collectées ; les finalités de la collecte des données ; les destinataires des données ; les droits des clients ; les mesures de sécurité mises en place pour protéger les données.

3. Réaliser une analyse d'impact sur la protection des données (PIA)

Réaliser une analyse d'impact sur la protection des données (PIA) afin d'évaluer les risques liés à la collecte et au traitement des données personnelles des clients. Elle peut être réalisée par un expert en protection des données.

La PIA doit notamment identifier les risques suivants : la perte ou la destruction des données ; la divulgation ou la diffusion non autorisée des données ; la modification ou la corruption des données

4. Mettre en œuvre des mesures de sécurité

Mettre en œuvre des mesures de sécurité pour protéger les données personnelles des clients. Ces mesures doivent être adaptées aux risques identifiés dans la PIA.

Les mesures de sécurité mise en œuvre comprennent notamment les suivantes : la mise en œuvre de protections (antivirus, firewall) performants ; l'utilisation de mots de passe forts ; la mise en place d'un système de sauvegarde des données ; la limitation de l'accès aux données aux personnes autorisées

5. Informer les clients

Les clients doivent être informé des modalités de collecte et de traitement de leurs données personnelles. Cette information doit être réalisée de manière claire et concise, et doit être accessible aux clients. Ces informations sont généralement placées dans une page spéciale accessible à partir de la page d'accueil du site Web de l'entreprise.

Les informations suivantes doivent être communiquées aux clients : les données personnelles collectées ; les finalités de la collecte des données ; les destinataires des données ; les droits des clients ; les mesures de sécurité mises en place pour protéger les données.

Mission 4 – Gérer les procédures de sauvegarde et la charte informatique de l'entreprise		Erbioline
Durée : 1 h 20'	ou	Source

Contexte professionnel

La société ***Erbioline*** est gérée par **Camille Berthod** qui en est PDG. Elle conçoit des parfums, déclinés en crèmes et savons qu'elle fait fabriquer à Grasse, (Var), pour les parfums et à Venise pour les crèmes et savons. Elle reçoit les produits transformés et assure l'empaquetage et le packaging. Son activité est donc la suivante : achats ventes de parfums, savons, crèmes, achats ventes d'accessoires : rouges à lèvres, brosses…, création de parfums personnalisés, création d'ambiance olfactive pour l'évènementiel.

M^me^ Berthod et le responsable informatique souhaitent imposer des règles communes de fonctionnement concernant les sauvegardes informatiques et l'utilisation de l'informatique dans l'entreprise.

Travail à faire

1. Rédigez la **note de service** qui expliquera les nouvelles procédures de sauvegarde et d'utilisation de l'informatique de l'entreprise à l'aide des consignes qui vous sont remises dans le **document 1**.
2. Concevez la fiche de contrôle des sauvegardes qui sera placée dans le dossier **« sécurité »** de l'espace partagé du serveur. Après chaque sauvegarde, il faut mettre à jour la fiche qui récapitule la date, le nom de la personne qui a fait la sauvegarde et le numéro de l'ordinateur.
3. L'information concernant la description des incidents informatiques qui interviennent dans l'entreprise est aléatoire et nécessite souvent des rappels pour préciser différents points à prendre en compte. Concevez sur un texteur une fiche d'incident destinée à collecter les informations concernant les incidents informatiques en vous aidant des informations remises dans le **document 2**.

Doc. 1 Consignes de M^me^ Berthod et du responsable informatique

Les points suivants devront être indiqués :

Le serveur principal possède deux disques de sauvegarde (J:) et (K:)
- le disque **(J :) Serveur** sauvegarde tous les soirs le contenu du disque du serveur principal,
- le disque **(K:) Sauvegarde** est dédié à la sauvegarde des contenus des disques de chaque ordinateur. Chaque responsable d'ordinateur devra réaliser une sauvegarde du contenu de son disque dur sur le disque K : du serveur tous les vendredis soir.

Une **fiche de contrôle** des sauvegardes sera placée dans le dossier **«** Sécurité » de l'espace partagé du serveur. Après chaque sauvegarde, il faut mettre à jour la fiche qui récapitule la date, l'heure, le nom de la personne qui a fait la sauvegarde et le numéro de l'ordinateur

Fonds d'écran : le fond d'écran des ordinateurs devra afficher le logo de la société. *Vous rappellerez le mode opératoire dans l'annexe de la note de service.* Le logo est accessible à partir du dossier **Logo entreprise** du serveur.

Écran de veille : pour lutter contre les personnes trop curieuses, des écrans de veille devront s'activer sur tous les ordinateurs au bout de 7 minutes d'inactivité. L'écran devra afficher un texte en 3D rappelant le nom de la société. *Vous rappellerez le mode opératoire dans l'annexe de la note de service*.

Autres points : vous devrez définir les règles applicables en ce qui concerne les points suivants :
- téléchargement de films et musiques non professionnels (interdit) ;
- installation de nouveaux programmes (interdit) ;
- utilisation d'Internet dans le cadre non professionnel (toléré en dehors des heures de travail avec respect de la légalité et des bonnes mœurs) ;
- Utilisation des courriels (mêmes règles que pour l'utilisation d'Internet) ;
- L'usage d'Internet ne peut pas nuire à l'image de l'entreprise, même si c'est dans un cadre privé.

Vous rappellerez que ces règles et procédures sont mises en œuvre dans l'intérêt de tous et que tout manquement à ces règles de sécurité ne saurait être accepté.

Doc. 2 Informations indispensables

La fiche doit indiquer :

- La nature du problème : logiciels ou matériels ;
- Le numéro du client et le N° du contrat de maintenance ;
- Le nom de la personne qui a appelé et qu'il faut recontacter ainsi que son numéro de ligne directe ;
- Si le problème à déjà été rencontré ;
- La date, l'heure et le poste sur lequel le problème est apparu ;
- La situation actuelle du réseau et le niveau d'urgence de la réparation (Le réseau est bloqué, un seul poste est bloqué, l'imprimante est bloqué) ;
- Le délai d'intervention souhaité pour la réparation ;
- S'il y a un message d'erreur affiché à l'écran (rappeler dans la fiche la procédure permettant d'imprimer une fenêtre de message ([Alt] + [Impr. écran] puis coller l'image sous Word par [Ctrl] + [V]).

Mission 5 – Auditer la sécurité informatique d'une PME		Erbioline
Durée : 50'	ou	Source

L'objectif de cet exercice n'est pas d'apporter des solutions à tous les risques informatiques, mais de faire réfléchir à la diversité des risques encourus par l'entreprise et de mener une pré-réflexion sur les solutions possibles.

Contexte professionnel

M^me^ Berthod a découvert qu'un nouveau produit conçu pour répondre à un appel d'offres a été piraté par un concurrent qui a proposé un produit très proche. Elle vous demande de réaliser un audit des risques informatiques supportés par la société.

Travail à faire

Complétez le tableau des risques informatiques encourus par la société, à partir de la description de l'organisation de la société qui vous est remise dans le **document 1**.

Identification des risques	Protection existante	Personnel concerné	Action(s) à envisager
Panne électriques			
Panne serveur			
Perte de données			
Virus			
Accès malveillant			
Espionnage			
Vol de matériel			

Doc. 1 Organisation de la société

1. Prestation fournie

La société fabrique les produits qu'elle commercialise. Pour cela, elle possède un bureau d'étude, un service de production et un service commercial.

Elle commercialise ses produits dans toute le France ; elle s'appuie, pour cela, sur son système informatique qui lui permet de réagir rapidement aux commandes et aux demandes des clients.

2. Structure de la société

- **Organigramme :** secrétariat - service commercial - bureau d'études - comptabilité/finances – directeur.
- **La direction** est composée de la directrice qui fait office de « directeur informatique ».
- **Le secrétariat** est animé par un attaché de gestion qui effectue également l'accueil téléphonique. Il dispose d'un ordinateur équipé d'une suite bureautique - messagerie (connecté au serveur).
- **Le service commercial** est composé de deux personnes qui créent et gèrent les dossiers clients. Seul, le service commercial est habilité à traiter avec l'extérieur ; il est donc garant de l'image de marque de l'entreprise. Il échange fréquemment des informations avec le bureau d'études (demande des clients, nouveau produit des concurrents), avec la comptabilité (prix) et avec l'extérieur (devis avec les clients).
- **Le bureau d'études** compte deux ingénieurs qui réalisent les activités suivantes :
  - ils cherchent de nouveaux produits ;
  - ils établissent des recherches de qualité quant aux normes sanitaires.
- **Le service comptabilité/finances** est chargé de la comptabilité. Il est composé d'une seule personne qui traite également les contentieux.

3. Clientèle

La clientèle est composée de particuliers, de chaines de magasin et de groupements d'achat.
Les statistiques montrent que les périodes de pointe se situent en novembre-décembre, avril-mai et l'été.

4. Structure informatique

- **Matériel :** voir le schéma du réseau.
- **Logiciels :** la société a acquis le logiciel Cosmetix pour l'aide à la création des différents produits et accède via un abonnement Internet à la base de données Biosanit pour connaître les caractéristiques des composants utilisés dans la fabrication des produits. Tous les postes sont équipés de logiciels de bureautique. Le système d'exploitation est Windows Server.

5. Sécurité

5.1 Sécurité du système d'information

Il n'y a pas de politique de sécurité particulière, seulement quelques règles :

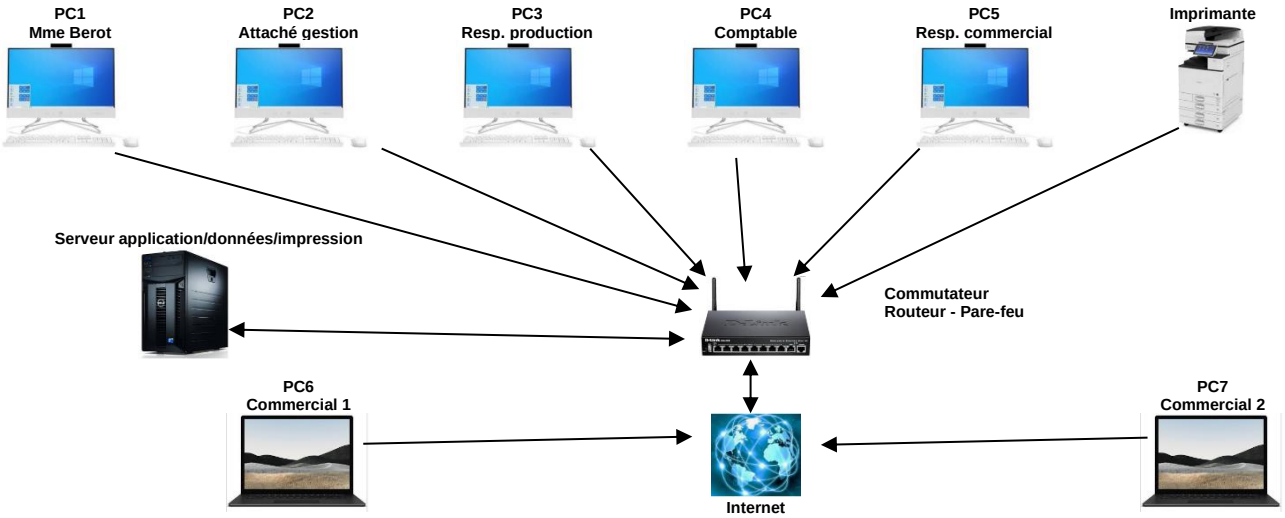
- le contrôle d'accès se fait par identifiant/mot de passe ;
- tous les fichiers sont sauvegardés sur le disque dur du serveur ;
- chaque membre du bureau d'étude est responsable du fichier qu'il traite ; les fichiers sont sauvegardés sur clé USB puis dans une armoire fermée à clé, située dans le bureau d'études ;
- parallèlement, les documents papiers sont rangés dans une armoire forte du service commercial ;
- en ce qui concerne la maintenance, un contrat a été établi avec les fournisseurs de logiciels avec intervention sous 12 heures.

5.2 Sécurité générale

Nous avons recueilli les informations suivantes :

- les moyens réglementaires de lutte contre l'incendie sont en place ;
- il existe des consignes de fermeture à clé des locaux, mais aucun moyen, ni procédure de contrôle n'a été mis en place ;
- le bureau d'étude et le service commercial sont climatisés ;
- une alarme anti-intrusion est active durant les heures de fermeture (19 h-7 h) ;
- Les salariés commencent à travailler à 8 h ;
- le service de nettoyage intervient de 7 h à 8 h ;
- la direction est située au premier étage d'un immeuble qui se trouve en bord de ville ; le bureau d'étude et le service commercial sont au rez-de-chaussée, les fenêtres sont sans protection particulière mise à part une fermeture par des volets roulants ;
- le bureau du directeur est le seul à bénéficier d'une clé de sécurité qu'il détient ;
- les clients sont reçus dans le bureau des commerciaux, mais il arrive que des visites aient lieu au bureau d'études (lord des démonstrations par exemple) ;
- le serveur central est situé dans une pièce isolée, contiguë au bureau d'études et bénéficie d'une alimentation secourue. C'est dans cette pièce que sont également disposées les imprimantes.

6. Organisation informatique



Mission 6 – Évaluer une solution en cloud computing		Signaux Girault
Durée : 50’	ou	Source

Contexte professionnel

La société Signaux Girault conçoit des systèmes de signalisation lumineux reposant sur l’intégration des technologies LED dans des panneaux lumineux. Les salariés sont répartis dans trois divisions : enseigne, signalisation, sécurité.

Le service informatique (SI) emploie deux personnes à temps plein. Il gère le réseau informatique, les sauvegardes de données et l'installation et la maintenance des logiciels professionnelles et bureautique. La sauvegarde des données est assurée sur un serveur interne qui est dupliqué en Cloud externe auprès de la société Dell.

M^me^ Girault n'est pas satisfaite du SI. Elle estime son coût trop élevé. Par ailleurs, l'installation et la maintenance des matériels et des logiciels sont la source régulière de conflits entre le personnel et les informaticiens.

Elle envisage de supprimer la sauvegarde interne qu’elle juge inutile pour ne conserver que la sauvegarde externe auprès de la société Dell dans la mesure où cette dernière garantie contractuellement une sécurité complète des données en datacenter sans coût supplémentaire. Elle souhaite également recourir à la solution bureautique en ligne proposée par Google. Cependant elle s’interroge sur la pertinence de recourir à deux prestataires en Cloud (Dell et Google) et sur le coût de la solution proposée par Google.

Travail à faire

1. Expliquez dans une note, à l’aide du **document 1**, en quoi consiste le multicloud et ses avantages pour l’entreprise.
1. Chiffrez le coût de la mise en œuvre de Google Workspace business dans l’entreprise à l’aide des **documents 2** et **3**, sachant que l’ensemble du personnel l’utilise à l’exception des techniciens de production. Dans ce contexte un emploi serait supprimé au service informatique (salaire brut 2 400 € par mois, les charges patronales représentent 35 % du brut).

Doc. 1 Qu’est-ce que le multicloud ?

Source : www.delltechnologies.com

Parallèlement à l’évolution des offres Cloud au cours de la dernière décennie, les entreprises ont de plus en plus adopté des services multiclouds au lieu d’avoir recours à un seul fournisseur de Cloud. Les environnements multiclouds permettent aux entreprises de choisir parmi des solutions de pointe, car elles décident de l’emplacement d’exécution des applications et des charges applicatives.

Qu’est-ce que le multicloud Computing ?
Le multicloud Computing fait référence à l’utilisation de plusieurs services Cloud plutôt que d’un seul prestataire de services Cloud. Un environnement multicloud utilise généralement au moins deux services de Cloud public (fournis par des prestataires tiers). Les environnements multiclouds peuvent également inclure un Cloud privé (interne à l’entreprise) qui implique la technologie Cloud qui réside dans le propre datacenter de la société.

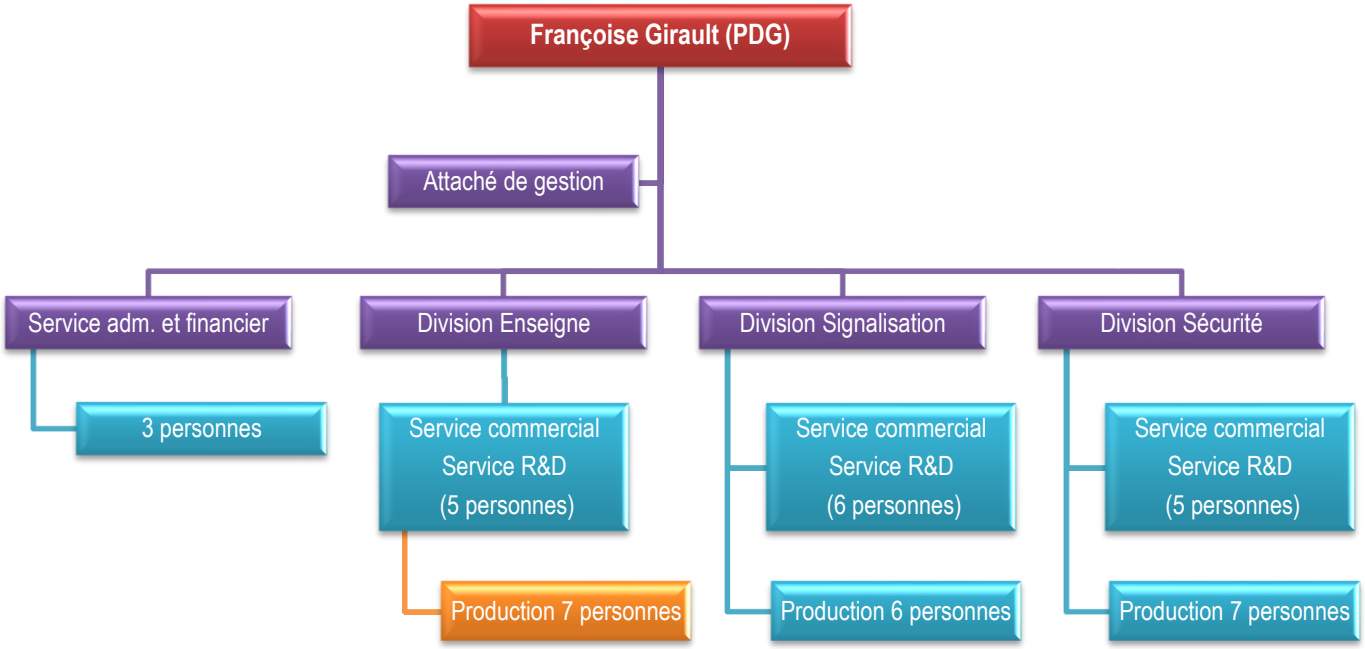
Quels sont les objectifs des environnements multiclouds ?
Avec l’infrastructure multicloud, les équipes IT peuvent exécuter des charges applicatives individuelles sur le service Cloud afin d’améliorer l’efficacité des applications et de réduire les coûts.

Quels sont les avantages d’un environnement multicloud pour les entreprises ?
Les environnements multiclouds permettent aux entreprises de réduire les coûts et d’équilibrer de manière optimale les dépenses en capital et les dépenses d’exploitation lors de l’acquisition des services Cloud. Ainsi, les entreprises peuvent innover plus rapidement tout en apportant une différenciation à leurs clients.

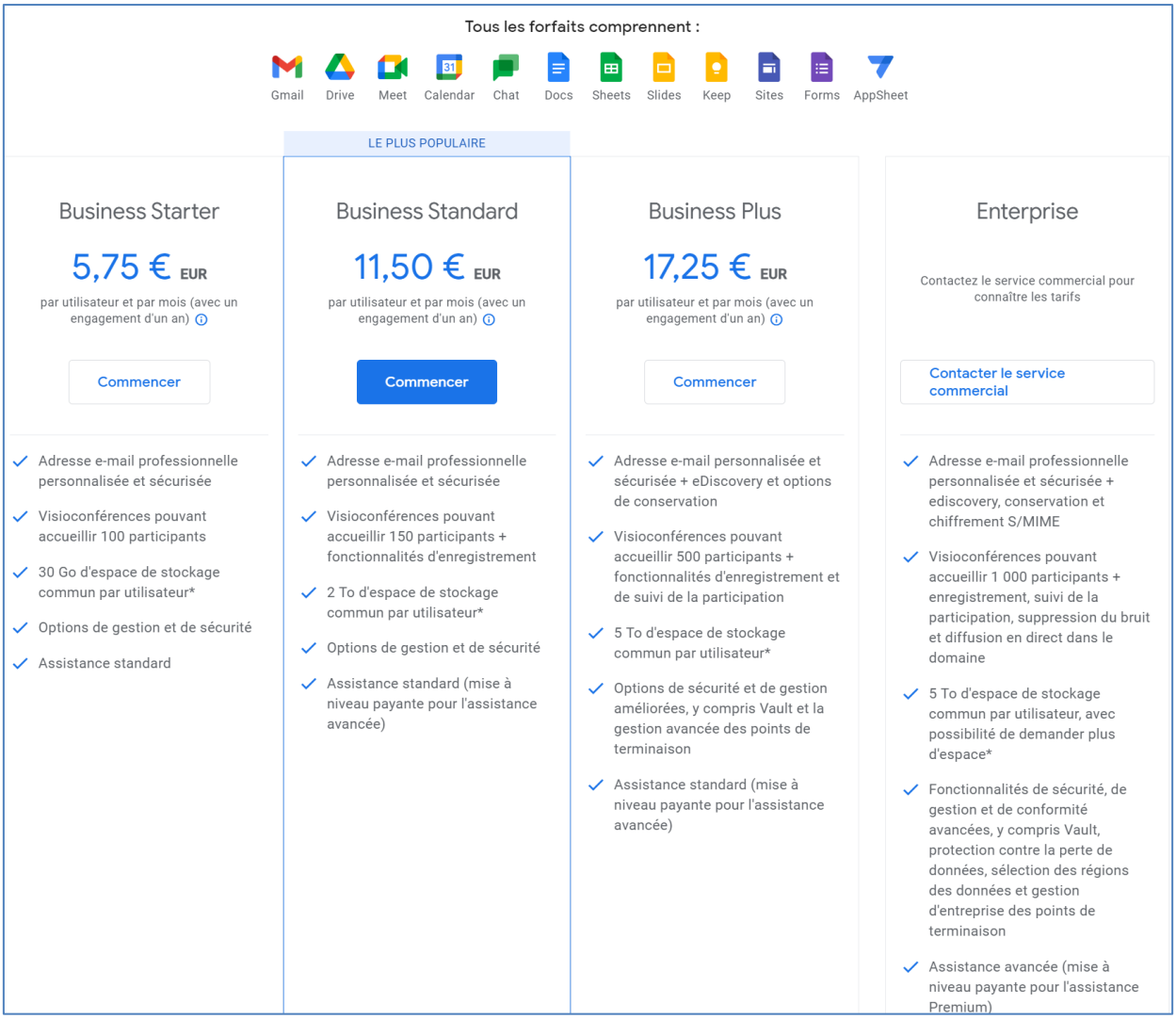
Quels sont les avantages d’un environnement multicloud pour les équipes IT ?
Pour les équipes IT, une infrastructure multicloud améliore l’efficacité des applications et la capacité à répondre aux besoins en temps réel de l’entreprise.

Quelles sont les difficultés liées à un environnement multicloud ?
Chaque service Cloud est accompagné de son propre ensemble d’outils de gestion, de processus, de contrats de niveau de service et de difficultés en matière de sécurité. Lorsque les équipes IT sont chargées de la gestion de plusieurs services Cloud, le basculement entre les plates-formes peut rapidement devenir chronophage et fastidieux, entraînant alors des risques supplémentaires, car les administrateurs doivent configurer plusieurs instances Cloud tout en assurant une sécurité appropriée pour chacune d’elles. La portabilité des données et des applications est également plus complexe, ce qui ajoute une charge de gestion supplémentaire et limite la vitesse et l’innovation.

Doc. 2 Organisation de la société



Doc. 3 Solution Google Workspace



Ressources

1. Gérer le système d'information : le système informatique

1.1. Le système d'information

Toute organisation génère de l'information et son bon fonctionnement repose sur une bonne gestion de ces dernières. Le **S**ystème d'**I**nformations (**SI**) d'une entreprise correspond à un ensemble organisé de ressources destinées à collecter, traiter, stocker puis diffuser ses informations. Le SI fait largement appel aux technologies de l'information et de la communication (TIC) pour en permettre une gestion efficace et sécurisée.

Le SI a principalement deux finalités, **fournir des informations aux dirigeants** pour piloter la société *(tableaux de bord, statistiques…)* et **mettre en œuvre la gestion quotidienne** *(achats, facturations, paie, production…)*.

Ces informations sont variées et multiples et proviennent de l'environnement **externe** de la société (lois, économie, marché, concurrents, fournisseurs, clients, internet…). Elles proviennent également de son activité **interne** (production, recherche, achats, ventes… de son organisation, des techniques et procédures mises en œuvre, de son personnel…).

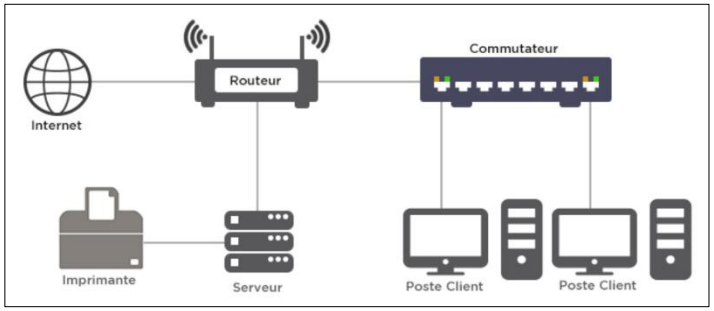
1.2. Le système informatique

La quantité d'informations à gérer est de plus en plus grande.

Cette gestion fait largement appel à l'informatique qui permet de stocker et de traiter rapidement de grandes masses d'informations. L'informatisation est mise en œuvre à l'aide d'ordinateurs reliés en réseaux qui utilisent des applications destinées à assurer un fonctionnement sécurisé du système et un traitement efficace des données.

2. Les réseaux informatiques

Un réseau informatique est un ensemble de moyens matériels et logiciels destinés à faciliter la communication et le partage des ressources. Il repose sur des composants matériels connectés à l'aide de liens filaire (câble Ethernet) ou non filaire (Wi-Fi, 4G, 5G). Chaque élément du réseau est identifié par une adresse IP différente.



Avantages et inconvénients d'un réseau	
Avantages	**Les ressources sont partagées** : le matériel *(imprimante, scanneur, modem, disque dur…)* ; les applications ; les fichiers et bases de données ; les accès à Internet. ⇨ ce qui réduit les investissements et des coûts de maintenance.
	Le système d'exploitation server permet de paramétrer des droits d'accès au réseau, aux espaces, aux dossiers, aux applications.
	Les fichiers sont échangés de poste à poste sans recourir à un support intermédiaire : *CD, clé USB...*
	Il facilite le travail collaboratif avec une messagerie commune, des agendas et des espaces partagés.
	Il facilite la gestion des sauvegardes centralisées et automatiques.
Inconvénients	Un réseau est **complexe à administrer** et son administration doit être confiée à un spécialiste. Par ailleurs les pannes sont très perturbantes pour l'organisation car tous les postes du réseau en sont victimes.

2.1. Le matériel

- **Poste ou terminal réseau**

Ce sont les ordinateurs (fixes ou portables) connectés au réseau à partir desquels les utilisateurs accèdent et utilisent les ressources du réseau (Internet, applications, fichiers, etc.).

- **Hub, switch, commutateur**

Il est relié à chaque élément du réseau. Il **reçoit**, **filtre** et **oriente les informations** vers les ordinateurs, serveurs, imprimantes ou Internet cibles.

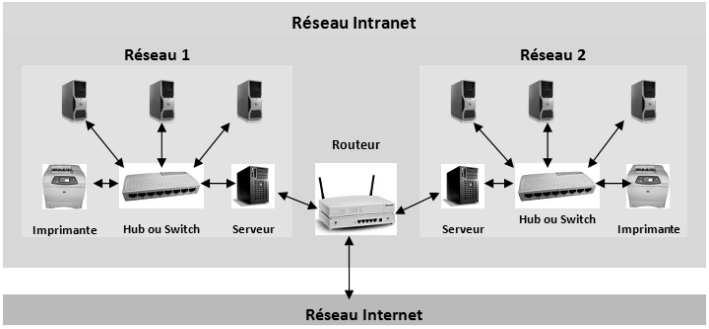
- **Serveur**

Cet ordinateur administre le réseau. Dans les TPE un serveur unique assure l'intégralité des tâches, mais dans les organisations plus complexes, des serveurs sont spécialisés dans des tâches particulières

Principaux serveurs	
Serveur d'administration	Il gère le réseau, les identifiants des postes, les connexions, les droits d'accès, les priorités…
Serveur d'applications	Il gère les applications (PGI, production, achats, ventes, bureautique…) et les droits d'accès.
Serveur de données (NAS)	Il stocke les fichiers et les données partagées : agenda, messagerie, bases de données, etc.
Serveur d'impression	Il gère les imprimantes, les files d'attente et les priorités d'impression.
Serveur Web	Il gère les accès internet, les sites Web, les messageries en lignes et les applications en Cloud.
Serveur de messagerie	Il gère les comptes de messageries, les envois et réceptions de courriels.

- **Routeur et Bridges**

Un réseau peut être divisé en sous réseaux afin de sécuriser le système en limitant les accès et les passerelles entre les réseaux. L'interconnexion de plusieurs réseaux nécessite un matériel spécifique appelé un pont (**bridge**) ou **routeur**.



- **Onduleur**

C'est un matériel qui protège le réseau contre les coupures de courant électrique en maintenant l'alimentation sur batterie pendant une durée plus ou moins longue selon sa puissance de l'onduleur.

- **Connecteurs**

Les connexions peuvent être filaire (Ethernet) ou sans fil (WIFI ou 5G)

- Prise Ethernet : chaque poste relié au réseau par cable coaxial est équipé d'une carte Ethernet disposant d'un port dans lequel vient se connecter une prise RJ45.

- Carte WiFi : les connexions par ondes WiFi évitent de câbler les bâtiments. Chaque poste possède une carte WiFi et le routeur doit également être un émetteur/récepteur WiFi.

- **Carte 4G ou 5G** : elles permettent de relier au réseau des tablettes ou des Smartphones.

***Adresse IP** : pour communiquer, chaque matériel relié au réseau (ordinateur, imprimante, etc.) est identifié par une combinaison de 4 chiffres compris entre 0 et 255, appelée **adresse IP** (Exemple : 192.168.133.25).*

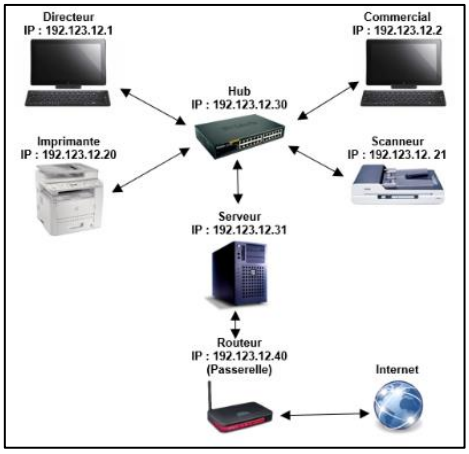
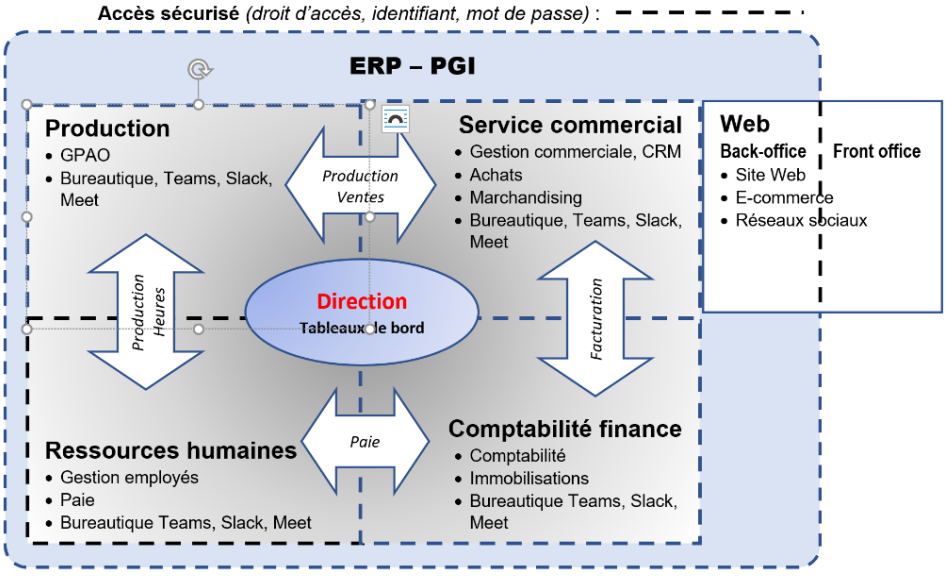


Schéma d'un réseau avec adresses IP

2.2. Les logiciels

L'informatique fonctionne à l'aide de programmes. Certains paramètrent le réseau ou l'ordinateur (système d'exploitation), d'autres protègent les matériels et les fichiers contre les actions malveillantes (virus, piratage, ransomware…) d'autres sont des utilitaires qui simplifient l'utilisation des ordinateurs (navigateurs, messagerie, lecteur pdf, transfert ou compression de fichiers…) et d'autres enfin sont des applications professionnelles qui permettent de réaliser les tâches de gestion quotidiennes.

Programmes	Caractéristiques
Système d'exploitation	- Le **système d'exploitation serveur** paramètre le réseau : les matériels connectés, les utilisateurs, les droits d'accès, les espaces personnels et collaboratifs, les logiciels, les imprimantes et les impressions… - Le **système d'exploitation de l'ordinateur** paramètre l'ordinateur, l'interface graphique, les préférences de l'utilisateurs…
Sécurité	- **Antivirus** : il scanne les entrées sorties de données et détruit ou bloque les virus ou autres logiciels malveillants. - **Firewall** : il contrôle les accès au port internet de l'ordinateur et bloque les accès hostiles ou indésirables.
Utilitaires	- **Navigateur internet** : il paramètre les **préférences** de navigation et permet de **naviguer** sur le Web et d'afficher les pages Web (Edge, Chrome, Opéra, Mozilla…), de gérer les favoris... - **Gestionnaire de courriers** : la gestion des courriels peut être réalisée : • à l'aide d'une **application locale** qui importe et export les méls vers un serveur de messagerie local : Outlook, Thunderbird… • à partir de **serveurs en ligne** : Outlook, Gmail, Hotmail, Yahoo, etc. - **Lecteur pdf** : il lit les documents sauvegardés dans ce format. Le plus connu est Adobe Reader**.** Les applications bureautiques sont capables de créer et de lire des fichiers pdf. - **Compression/décompression** : il compresse/décompresse les fichiers pour en réduire la taille (7-Zip, Win Zip, WinRAR…).
Applications bureautique et professionnelles	- **Pack Bureautique** : ils proposent des outils de création et de mise en forme de textes, tableaux, bases de données, diaporamas, etc. Les plus connus sont **Microsoft 365** (Word, Excel, Access, PowerPoint) ; **LibreOffice** (Writer, Calc, Impress, Base) et **Google Workspace** (docs, Sheets, slide, Forms) qui fonctionne en ligne (Cloud). - **Logiciels professionnels** : ils enregistrent les opérations qui résultent de l'activité de l'entreprise (achats, ventes, production, paie, comptabilité, contacts client, etc.). Ce peut être des applications dédiées à une activité (Ciel, EBP, Loop comptabilité, paie, gestion commerciale…) ou une application intégrée du type PGI (SAP, YourCegid, Sage X3…) 

3. Identifier les risques informatiques et leurs solutions

Virus et programmes malveillants		
Risques	**Problèmes**	**Solutions**
Virus **Ver (Worm)**	Un **virus** est un programme introduit dans l'ordinateur, par un fichier exécutable (.exe ou .bat) contaminé. Il est très souvent dissimulé dans une pièce jointe. Une fois dans l'ordinateur, il se reproduit et peut s'attaquer aux données et aux programmes. Le v**er** récupère les adresses des contacts et envoie des copies à tous les destinataires qui seront à leur tour infectés.	**Installer une suite antivirus avec une mise à jour automatique** des nouvelles souches qui analyse en temps réel tout fichier entrant et recherche les signatures virales éventuelles (plusieurs milliers de virus apparaissent chaque jour).
Rançongiciel **(Ransomware)**	C'est un logiciel rançonneur qui s'installe comme un virus en cliquant un lien ou une pièce jointe. Il crypte les fichiers et les rend inutilisables. Pour obtenir la clé de décryptage l'entreprise doit payer une rançon. **Il représente un risque majeur pour les entreprises car il bloque l'intégralité du système informatique.**	**Installer une suite antivirus qui intègre un module anti-ransomware.** - Sauvegarder régulièrement les données sur un disque dur externe ou en Cloud. - Ne pas cliquer un lien dans un mél dont la provenance n'est pas identifiée. - Détruire les messages suspects sans y répondre. - Ne pas exécuter d'instruction en provenance d'un inconnu.
Cheval de Troie **(Trojan)**	Un **« Cheval de Troie »** ouvre un port internet de l'ordinateur pour le rendre accessible à des hackers. Il facilite l'espionnage ou la prise de contrôle de l'ordinateur à distance.	**Installer une suite antivirus qui intègre un Firewall** qui filtre les données échangées et bloque les communications non autorisées.
Volonté de nuire		
Pourriel **(Spam)** **Hameçonnage** **(Phishing)**	Le **pourriel** est un courriel indésirable envoyé en masse à des fins publicitaires ou malhonnête. L'**hameçonnage** reproduit une page d'un organisme de confiance afin de soutirer des informations privées.	**Installer une suite antivirus** qui intègre un **anti-spam** et un **filtre anti hameçonnage**.
Spyware **(mouchard)**	Ces programmes recueillent des informations sur les habitudes de l'utilisateur puis les envoie à la société qui le diffuse pour le profiler.	**Installer une suite antivirus** qui intègre un **antispyware** qui recherche et détruit ces programmes.
Cookies	Ces fichiers, stockés sur l'ordinateur, enregistrent des habitudes de l'internaute. Lors d'une nouvelle visite, le site peut ainsi connaitre ses pratiques et personnaliser ses offres.	Programmer le navigateur Web pour qu'il interdise l'installation des **cookies**.
Hacker, **cracker**	Un **hacker** ou un **cracker** est une personne qui casse les codes d'accès des ordinateurs ou du réseau pour pénétrer un système informatique, par jeux ou par malveillance.	**Protéger les accès** (réseau, dossiers, applications, fichier) par des mots de passe forts.
Espionnage **Vol** **Sabotage**	L'entreprise doit anticiper les **malveillances** (vols, espionnage, sabotage…). Il doit notamment anticiper ses risques en cas de licenciement, de départ de la société, de procès, de conflits avec du personnel de la société.	- Protéger l'accès aux locaux par des serrures ou des systèmes biométriques (empreinte digitale ou rétinienne) ou par une clé électronique. - Le matériel doit être protégé contre le vol, les salles doivent être fermées et les ordinateurs attachés. - Bloquer l'accès aux ordinateurs par des mots de passe forts. - Sensibiliser le personnel aux risques.
Piratage sur les réseaux sans fil	Dans les **réseaux sans fil**, les données sont transmises par des ondes WiFi qui peuvent être interceptées par des personnes externes à l'entreprise.	Le modem WIFI doit être protégé par un mot de passe fort et les données transmises doivent être cryptées.

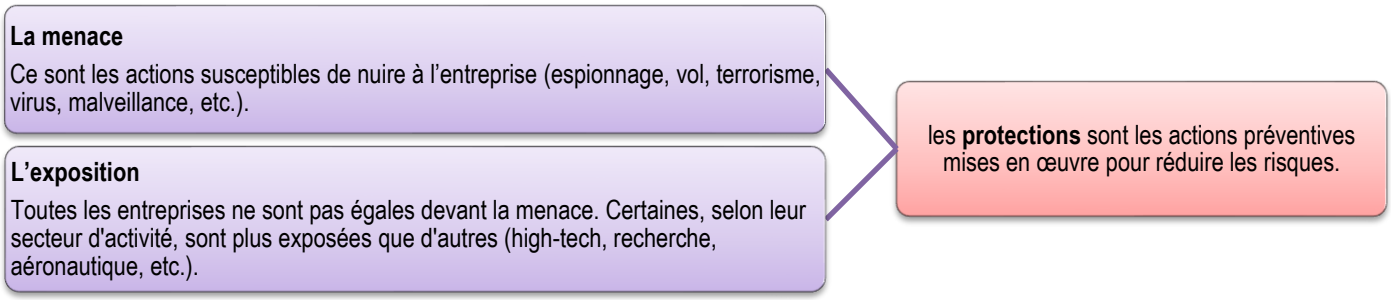
Accidents		
Panne de disque dur **Ransomware**	Un disque dur peut tomber en panne ou être détruit dans un incendie ou un dégât des eaux. Les données peuvent être perdues et la reconstitution des fichiers peut être longue et coûteuse. Le cryptage des données par un ransomware a les mêmes conséquences.	Réaliser des **sauvegardes régulières des données** sur un disque dur externe dans l'entreprise en automatisant les sauvegardes, en dehors des heures de travail, à l'aide du programme de gestion du serveur. Utiliser une **société spécialisée dans le Cloud computing** (Amazon Web Service ; Microsoft Azure ; Google cloud plateform ; OVH ; IBM ; Cisco…) qui sauvegardent constamment les données dans des datacenters ce qui réduit les risques de pertes.
Serveur cloud indisponible	Les sociétés de Cloud computing garantissent une disponibilité de leurs serveurs à 99,9 %. Mais le 0,01 % signifie une indisponibilité de plusieurs heures par an dont les conséquences peuvent se chiffre en millions d'Euros pour les sites commerciaux.	Le **recourt à plusieurs opérateurs en Cloud** (ou multicloud) permet de répartir les risques et de maintenir l'activité lorsqu'un service n'est plus disponible en transférant les opérations vers d'autres opérateurs.
Coupure de courant et foudre	Une coupure de courant peut endommager les fichiers ouverts et occasionner la perte des fichiers en cours de traitement.	Installer un **onduleur qui** maintient l'alimentation électrique en cas de coupures, microcoupures, surtensions, sous-tensions ou foudre.
Négligence	La négligence est difficile prévenir et peut prendre des formes multiples et inattendues. Les conséquences peuvent être graves pour l'entreprise. - Perte d'une clé USB, d'un ordinateur, d'une tablette, d'un smartphone dans un lieu public… - Oubli de formater un disque dur qui contient des données confidentielles lors d'un changement d'ordinateur. - Oubli de fermer la porte d'accès à une salle informatique ou de verrouiller l'ordinateur pendant une pause.	Sensibiliser le personnel aux règles de sécurité. Ne pas copier les fichiers lors des déplacements. Protéger son ordinateur portable contre le vol. Mettre des protections destinées à interdire l'accès à l'ordinateur, etc.

4. Mettre en œuvre la sécurité informatiques au quotidien

4.1. Sensibiliser les utilisateurs à la sécurité informatique

Les risques informatiques ont souvent pour origine une négligence ou un acte malveillant dont les conséquences peuvent être dramatiques pour la société. Celle-ci doit impérativement mettre en place une politique volontariste destinée à prévenir ces risques. Il n'existe pas de solution universelle et des parades doivent être adaptées à chaque risque identifié.

La gestion des **risques** dépend de la **menace** et de **l'exposition** qui justifieront l**es protections** à mettre en œuvre.



Les contremesures peuvent être **des solutions techniques** *(antivirus, pare-feu, mot de passe, cryptage…)*, mais encore des **procédures** à respecter ou des **formations** et **sensibilisations** aux risques.

Plusieurs actions peuvent être envisagées : rédiger une charte informatique ; mettre en place des outils d'information ; former le personnel ; réaliser des tests.

- **Rédiger une charte informatique**

La charte informatique est un document qui précise les règles et les bonnes pratiques à mettre en œuvre par les utilisateurs des **matériels** (ordinateurs, smartphones, imprimantes) ; des **applications** (logiciels administratifs, logiciels de gestion, applications métiers, services en ligne) ; d'**Internet** ; des **téléphones** et de tout autre outils numériques (courriels, accès au réseau, partage de fichiers, vidéo-conférences, etc.)

La charte informatique intègre également des parties consacrées :
- à la mise en œuvre du télétravail et de la mobilité (travail à distance, voyage professionnel) ;
- aux aspects juridiques et au respect du Code du Travail et de la RGPD.

La charte informatique peut être annexée au contrat de travail ou au règlement intérieur de l'entreprise.

Sa rédaction nécessite des compétences techniques et réglementaires. Elle peut être réalisée à l'occasion d'un audit du système informatique et d'une évaluation méthodique des risques.

- **Mettre en place des bulletins d'information**

Une information régulière du personnel soutient sa sensibilisation aux bonnes pratiques. Ce peut être :
- un guide destiné aux nouveaux salariés, pour installer les bonnes pratiques dès leur entrée dans l'entreprise ;
- la diffusion de brochures de l'ANSSI (agence nationale de la sécurité des systèmes d'information), de la CNIL ou d'autres organismes ;
- la diffusion d'un bulletin d'information sur l'actualité et les protocoles à respecter en ce qui concerne : les mots de passe ; les mises à jour ; l'hameçonnage ; les rançongiciels ; les sauvegardes ; les usages personnels et professionnels ; les usages en mobilité et télétravail ; les réseaux sociaux…

- **Mettre en place des formations**

Le manque de compétences ou de connaissances est une source de risques informatiques. La formation du personnel peut réduire ce risque. Ces formations peuvent être prises en charge sur le budget de la formation professionnelle.

Elles peuvent aborder différents aspects de la sécurité informatique :
- le postes de travail, risques Internet, travail à distance… ;
- les bonnes pratiques et usages (mises à jour, sauvegardes…) ;
- les comportements à adopter en cas d'imprévues (fraude à l'identité, réaction en cas d'attaque informatique…)

- **Réaliser des simulations d'intrusion**

Cette action consiste à tester les employés en situation réelle pour vérifier qu'ils adoptent les procédures recommandées. Ce peut être des simulations d'intrusion ou de phishing, l'envoi de méls de sources inconnues pour voir si les personnes les ouvrent ou cliquent des liens intégrés au courriel…

Pour ces tests l'entreprise peur recourir aux services d'un prestataires extérieur.

4.2. Choisir un mot de passe

L'efficacité d'un mot de passe est indissociable de son utilisateur. Il est donc très important de choisir des mots de passe difficiles à retrouver à l'aide d'outils automatisés et difficiles à deviner par une tierce personne.

Méthodes d'attaque des hackers

Lors d'une attaque, les hackers utilisent des logiciels qui génèrent des mots de passe, jusqu'à une authentification réussie. D'où l'importance de limiter le nombre de tentatives. Dans ce cas, ces attaques sont quasi impossibles.

Les hackers utilisent principalement 2 techniques pour forcer un mot de passe.

⇨ **L'attaque par ingénierie sociale** : elle consiste à deviner le mot de passe, en fonction d'éléments personnels du propriétaire (nom, prénom, date de naissance…). Ces éléments sont ajoutés au logiciel de hackage qui cherche le mot de passe en faisant varier les combinaisons autour des mots retenus. *(Exemple : ajout d'un ou plusieurs chiffres, avec ou sans majuscules, remplacement des caractères par des chiffres, etc.).* Un mot de passe sans référence à un mot connu rend cette attaque inopérante.

⇨ **L'attaque brute** : les hackers utilisent des logiciels qui génèrent des mots de passe aléatoires. Plus le mot de passe contient de caractères et plus les types de caractères sont variés, plus cette attaque mettra de temps à aboutir.

Il n'existe pas de mot de passe infaillible, c'est la complexité de la recherche qui le rend plus ou moins fiable.

- **Les mots de passe forts**

Choisir un mot de passe
• Il doit faire plus de 8 à 10 caractères. • Il doit être composé de minuscules, majuscules, lettres, chiffres et caractères spéciaux. • Il ne doit pas avoir un lien avec soi : nom des enfants, du chien, date de naissance, de mariage, etc. • Il doit être unique et ne pas concerner différents accès. • Il doit être modifié régulièrement. • Il ne doit pas être enregistré par les applications ou les sites. • Il ne doit pas être noté dans un fichier ou sur l'ordinateur. • Si possible, limiter le nombre de tentatives d'accès.

- **Choisir et retenir un mot de passe fort**

Un mot de passe trop compliqué est difficile à retenir, et sera souvent écrit sur un bout de papier à côté de l'ordinateur. Il est conseillé d'utiliser des moyens mnémotechniques pour fabriquer et retenir facilement un mot de passe :
- **Méthode phonétique** : « J'ai acheté 3 CD pour cent euros cet après-midi » : **ght3CDp%E7am** ;
- **Méthode des premières lettres** : « La vie vaut elle d'être vécue mon amour » : **LVVEDEVMA**

Il est possible de décliner plusieurs mots de passe à partir d'un mot de passe fort, en changeant, par exemple, l'un des caractères de celui-ci. Il est ainsi plus facile de retenir des mots de passe différents.

4.3. Sauvegarder les données

Les données enregistrées dans les disques durs doivent faire l'objet de sauvegardes constantes afin de prévenir tout problème matériel ou autres qui pourraient entraîner des conséquences catastrophiques pour l'entreprise.

- **Quels fichiers sauvegarder ?**

Sauvegarder tous les dossiers et fichiers de données qu'il ne faut pas perdre en cas de défaillance du disque et du système, à l'exception des applications qui peuvent être réinstallées.

Les entreprises qui fonctionnent en Cloud (sauvegarde en ligne) et en mode SaaS (applications en ligne), n'ont plus à se préoccuper des sauvegardes. Elles sont gérées par l'entreprise de services Web qui garantit par contrat des sauvegardes constantes.

- **Types de sauvegarde**

Sauvegarde complète	Manuelle ou automatique, elle consiste à copier périodiquement l'intégralité les données d'un disque ou d'un dossier sur un deuxième disque. Cette technique présente cependant des inconvénients : - La copie de l'intégralité des données, peut être très longue ; - Elle conduit à recopier des fichiers qui n'ont pas été modifiés depuis la dernière sauvegarde ; - La sauvegarde dépend d'une opération volontaire qui reste soumise au risque de l'oubli ; - Les modifications réalisées entre deux sauvegardes sont perdues.
Les solutions suivantes sont les plus utilisées. Elles consistent à relier le disque source à un ou des disques durs externes (dans l'entreprise ou en Cloud) qui fonctionnent en mirroring (Ils sont, en continu, le miroir du disque source).	
Sauvegarde incrémentale	C'est une sauvegarde automatique qui intervient après une première sauvegarde complète. Seuls les fichiers ayant été modifiés ou ajoutés depuis **la dernière sauvegarde** sont sauvegardés. Cette sauvegarde réduit le besoin de stockage, mais nécessite de posséder les sauvegardes précédentes pour reconstituer la sauvegarde complète.
Sauvegarde différentielle	C'est une sauvegarde automatique qui intervient après une première sauvegarde complète. Seuls les fichiers qui ont été modifiés ou ajoutés depuis **la dernière sauvegarde complète** sont sauvegardés. Cette sauvegarde est plus lente et plus exigeante en espace de stockage qu'une sauvegarde incrémentale mais elle est plus fiable car seule la sauvegarde complète est nécessaire pour reconstituer les données sauvegardées.

- **Logiciels de sauvegarde**

Il est déconseillé de réaliser manuellement les sauvegardes. Tous les systèmes d'exploitation incluent une application de gestion des sauvegardes et tous des fabricants de matériel de stockage incluent des logiciels de sauvegarde avec leurs produits.

5. Respecter la RGPD, le Governance Act et le Data Act

La **RGPD** (Règlement Général sur la Protection des Données) encadre le traitement des données personnelles dans l'Union européenne. Elle oblige les **entreprises** européennes à mettre en place les mesures de sécurité destinées à assurer une sécurisation maximale de l'intégrité des données personnelles stockées dans le système d'information.

Le règlement général de protection des données, UE 2016/679 émane d'une décision du Conseil et du Parlement européen et renforce la protection des données personnelles, simplifie la réglementation pour les entreprises. Il a trois objectifs :

Les avantages du cadre européen

Le RGPD tire avantage de l'harmonisation et de l'extraterritorialité du droit européen.
⇨ Les habitants et les organismes de l'UE en profitent à large échelle.
⇨ Il concerne notamment les filiales des entreprises européennes installées dans les pays tiers.

5.1. Les principes de base

• La transparence

Un site internet qui collecte des informations doit indiquer clairement : pourquoi il collecte des données ; comment elles seront utilisées ; combien de temps elles seront conservées et les tiers qui y auront accès. Ces informations doivent être écrites d'une façon concise, lisible et dans un vocabulaire simple. Le consentement doit être un acte positif et ne doit pas être une case cochée par défaut qu'il faut désactiver.

• Le droit des utilisateurs

Chaque utilisateur bénéficie :
- d'un **droit d'accès** à ses données (formulaire, adresse électronique, courrier...) ;
- d'un **droit à** l'oubli (photos ou informations gênantes) ;
- d'un droit à l'effacement (lorsqu'on quitte un site d'e-commerce...) ;
- d'un **droit au déférencement** sur un moteur de recherche. Comme pour la téléphonie mobile, il existe un droit à la portabilité : une fois vos données récupérées, vous pouvez les transmettre à un autre site.

• La responsabilité des entreprises

Chaque entreprise est responsable des données qu'elle récolte et de celles transmises à des sous-traitants. Elle doit prouver qu'elle a mis en place tous les moyens adéquats pour protéger ces données et sur ce qui est pertinent de collecter ou non.

En cas de violation des données (piratage, fuite...), l'entreprise doit le signaler aux victimes et aux autorités compétentes, dans les 72 heures.

En cas de manquement à ces obligations, les victimes peuvent se tourner vers la CNIL (Commission nationale de l'informatique et des libertés). Les sanctions peuvent aller jusqu'à 20 millions d'euros ou 4 % du chiffre d'affaires.

5.2. Mise en œuvre

La mise en œuvre se fait en plusieurs étapes, au cours desquelles l'entreprise peut faire appel à la CNIL ou à un prestataire extérieur pour être accompagné dans la démarche.

1. Nommer un délégué à la protection des données dans l'entreprise ;
2. Créer un registre des traitements des données réalisées dans l'entreprise. Il doit détailler les activités, les données utilisées et les personnes qui y ont accès et la durée de conservation des données ;
3. Trier les données et identifier les données nécessaires aux activités, les données sensibles à protéger en priorité et définir les protocoles d'accès à ces données ;
4. Justifier chaque donnée collectée, et informer les personnes sur la nature des données collectées, leur accès, leur durée de conservation et les modalités d'exercice du droit d'accès personnel.

5.3. Data Governance Act et Data Act

Ces deux réglementations européennes sont destinées à organiser et encadrer l'utilisation des données collectées par des organismes privés.

- Le **Data Governance Act** vise à faciliter la réutilisation des **données publiques** et détenues par des organismes privés. Il impose un cadre réglementaire pour les intermédiaires de données, qui facilitent la mise en relation des personnes qui disposent de données avec celles qui souhaitent les réutiliser. Il prévoit : la création d'un registre européen des intermédiaires de données, afin de garantir leur transparence et leur fiabilité ; l'obligation pour les

intermédiaires de données de respecter la protection des données personnelles ; l'établissement d'un cadre juridique pour la réutilisation des données, afin de la rendre plus facile et transparente.

- **Le Data Act** vise à favoriser l'utilisation des **données industrielles**. Il définit un cadre réglementaire pour le partage et la réutilisation des données par les entreprises, notamment les données produites par les machines et les objets connectés. Le Data Act prévoit notamment les mesures suivantes : le droit pour les entreprises de demander à leurs fournisseurs de données de leur fournir des données dans un format ouvert et lisible par machine ; le droit pour les entreprises de réutiliser les données qu'elles ont collectées auprès de leurs clients ou de leurs partenaires commerciaux, sous réserve du respect des droits des personnes concernées ; l'obligation pour les entreprises de prendre des mesures pour garantir la sécurité et la confidentialité des données qu'elles partagent ou réutilisent.

6. Travailler en Cloud computing

Le Cloud computing (ou informatique en nuage) consiste principalement à fournir, via Internet et un navigateur Web, des moyens de stockage dans des datacenters externalisés et des logiciels en ligne.

- **Stockage en ligne** : le Cloud offre de ressources évolutives et quasi illimitées tout en bénéficiant des capacités de sauvegarde et d'une grande sécurité en matière de gestion des données.
- **Logiciels en ligne** : ces applications, fonctionnent principalement en mode SaaS (Software as a Service).

Les leaders du marché sont essentiellement des sociétés américaines : Amazon Web Service (AWS), Microsoft Azure, Google cloud plateform, IBM, Cisco, Salesforce. Les prestataires hors USA sont principalement Alibaba (en Chine) et OVH (dans l'UE).

6.1. Stockage en ligne

Avantages	- L'entreprise n'a plus à acheter, installer et gérer les moyens de stockage en interne. Le stockage est externalisé et la maintenance des matériels est assurée par le prestataire ce qui réduit sensiblement le travail du service informatique de l'entreprise. - Ce service fait l'objet d'un abonnement auprès du prestataire internet. Le coût de l'abonnement est proportionnel au volume de stockage utilisé. - Cette solution est souple et évolutive, si les besoins évoluent à la hausse ou à la baisse, l'entreprise peut modifier le contrat à la demande. - Les bases de données sont accessibles en tout lieu et à tout moment dès lors que l'utilisateur dispose d'une connexion internet. C'est le prestataire qui gère les connexions. - Les sauvegardes sont assurées par le prestataire et les risques d'incidents sont quasiment inexistant notamment vis à vis des ransomwares.
Inconvénients	- L'entreprise doit disposer d'une bonne connexion Internet et l'accès est impossible lorsque la connexion est rompue. - Le fournisseur de services stocke les données de l'entreprise. Il doit être totalement fiable. - Afin de lutter contre le terrorisme, le Cloud Act américain autorise les USA à surveiller les contenus gérés par des entreprises américaines. Cela signifie que les données sensibles d'entreprise non américaines sont susceptibles d'être lues par des organismes d'État américain (CIA, NSA). Cela concerne (Amazon, Microsoft, Google, IBM…) que les données soient dans des Data Center installés sur le sol américain ou pas. Cette contrainte peut devenir majeurs pour les entreprises et les PME qui œuvrent dans des domaines sensibles. - Les abonnements garantissent un accès aux datacenters de 99,9 %. Les interruptions de service sont rares, mais peuvent durer plusieurs heures et entraîner des conséquences graves pour les entreprises de e-commerce et peuvent bloquer le fonctionnement de l'entreprise. - La réduction du travail du service informatique réduit les coûts et les effectifs du personnel dans ce service qui perd une partie de son pouvoir.

6.2. Logiciels en mode SaaS

Ces services ne sont pas forcément proposés par tous les prestataires mais c'est le cas notamment pour les applications bureautiques de Microsoft et de Google.

Avantages	- Les logiciels ne sont plus installés sur les serveurs de l'entreprise mais sont utilisés en ligne ce qui réduit les besoins en matériels et le travail du service informatique qui n'a plus à installer, paramétrer et assurer la maintenance des applications. - Les logiciels sont constamment mis à jour et les utilisateurs travaillent toujours sur les dernières versions. Tous les utilisateurs utilisant la même version des applications. - La facturation est proportionnelle au nombre d'utilisateurs. Le contrat peut être facilement adapté en fonction de l'évolution du personnel. - Les logiciels sont accessibles en tout lieu et à tout moment et avec différents types de matériels (ordinateurs fixes ou portables, tablettes, smartphone) dès lors que l'utilisateur dispose d'une connexion Internet.
Inconvénients	- L'entreprise est dépendante du prestataire et toute interruption de service bloque le travail des salariés même si ces problèmes sont exceptionnels. - Les coûts fixes d'achat des applications sont remplacés par des charges variables d'utilisation. l'entreprise doit vérifier sur le long terme la rentabilité des choix.

Chapitre 10 - La gestion des risques informatiques

Bilan de compétences

Compétences	Non acquis	Partiellement acquis	Acquis
J'identifie l'apport de l'informatique au système d'information	☐	☐	☐
Je connais les composants matériels des réseaux	☐	☐	☐
Je connais les composants logiciels des réseaux	☐	☐	☐
J'identifier les risques liés au virus et programmes malveillants	☐	☐	☐
Je connais les protections à mettre en œuvre contre les virus	☐	☐	☐
J'identifier les risques liés à la volonté de nuire	☐	☐	☐
Je connais les protections à mettre en œuvre contre la volonté de nuire	☐	☐	☐
Je connais les risques liés aux ransomwares	☐	☐	☐
Je sais comment se protéger contre les ransomwares	☐	☐	☐
J'identifier les risques liés aux accidents	☐	☐	☐
Je connais les protections à mettre en œuvre contre les accidents	☐	☐	☐
Je connais les règles de la sauvegarde informatique	☐	☐	☐
Je connais les différents types de sauvegarde existants	☐	☐	☐
Je sais parer aux problèmes matériels	☐	☐	☐
Je sais créer des mots de passe forts	☐	☐	☐
Je sais comment sensibiliser le personnel au risque informatique	☐	☐	☐
Je connais les règles liées à la RGPD	☐	☐	☐
Je connais les risques induits par un non-respect de la RGPD	☐	☐	☐
Je connais les risques induits à une mauvaise protection des données	☐	☐	☐
Je connais les caractéristiques du Cloud computing	☐	☐	☐
Je connais les avantages du Cloud computing	☐	☐	☐
Je connais les inconvénients du Cloud computing	☐	☐	☐
Je sais définir ce qu'est le mode SaaS	☐	☐	☐