

PPDT | PRÉPOSÉ CANTONAL À LA PROTECTION DES DONNÉES ET À LA TRANSPARENCE

Audit et secteur public: une expérience de terrain

Corinne Sauge, Présidente CeRFI SA



INTRODUCTION

En quoi consiste mon expérience?

Une expérience accompagnée

- Je pratique des **contrôles** (aussi appelés "audits") avec une **autorité** dans un autre canton depuis de nombreuses années.
- J'ai eu l'occasion de contrôler de **nombreuses organisations différentes**.



Interviews

- Ces contrôles consistent en différentes **interviews** des responsables des organisations "auditées":
 - **Direction**
 - **Administration - RH - Finances**
 - Au moins un **service opérationnel**
 - **Service informatique**



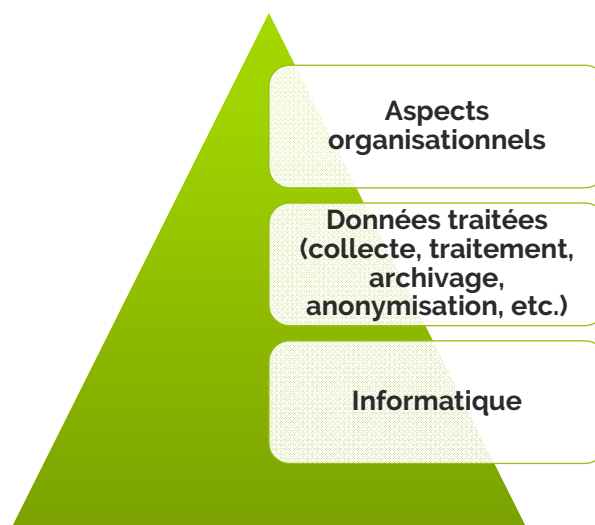
(C)CeRFI SA - 2016

5

Objectifs

- Vérifier le respect des **exigences légales** relatives à l'application de la protection des données.
- **Sensibiliser, informer et conseiller** sur la problématique de la protection des données, **dans un esprit de collaboration.**

Sujets traités



(C)CeRFI SA - 2016

6

Thèmes traités (1)

Accès à distance et physique	Anti-virus	Appareils portables et mobiles	Conservation et archivage	Autorité de surveillance
Classification	Données confidentielles	Données personnelles	Droits d'accès	e-mail
Formation	Support informatique	Imprimantes	Incendie / électricité	Internet

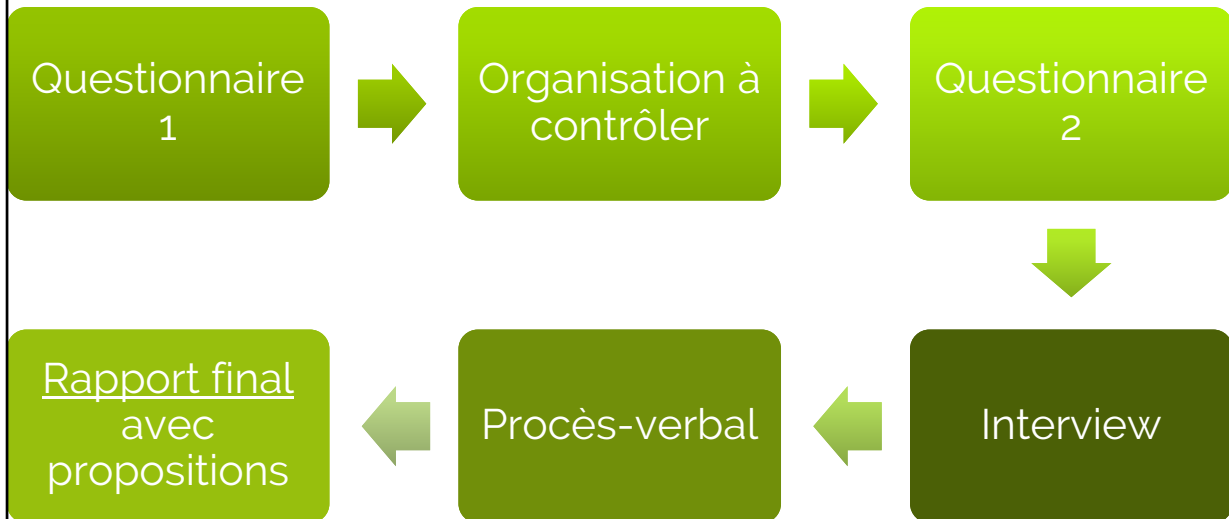
(C)CeRFI SA - 2016 7

Thèmes traités (2)

Locaux	Logiciels informatiques	Modes d'expédition	Mots de passe et autres mesures	Organisation
Panne / destruction	Place de travail	Poste de travail	Principe des 4 yeux	Réseaux sociaux
Responsables des données	Sauvegarde	Serveurs	Statistiques	Supports de données

(C)CeRFI SA - 2016 8

Méthodologie en bref



(C)CeRFI SA - 2016

9

Structure du rapport final



(C)CeRFI SA - 2016

10

Avantages de cette méthode

- **Personnalisation** des interviews
- **Contact direct** avec les responsables des organisations interviewées



(C)CeRFi SA - 2016

11



EXEMPLES DE QUESTIONS ET DE RECOMMANDATIONS

(C)CeRFi SA - 2016

12

QUESTIONS GÉNÉRALES

(C)CeRFi SA - 2016

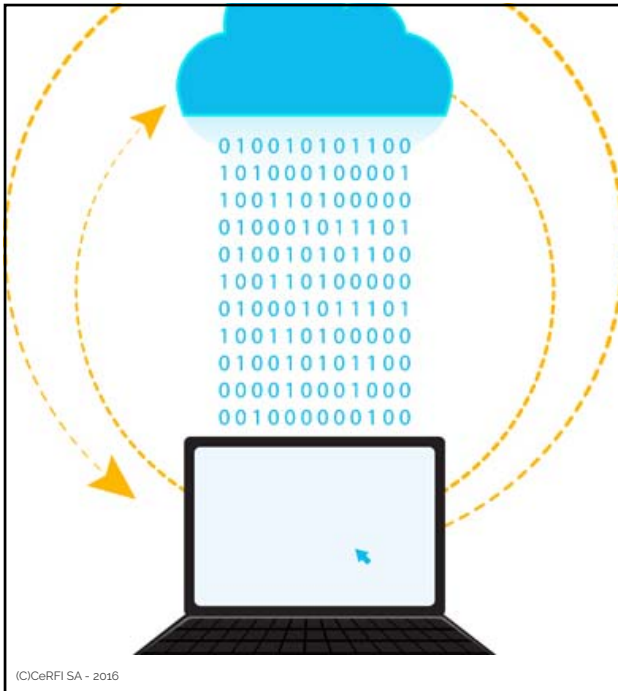
13

Organisation

- **Comment votre service est-il organisé?**
- Quelles **tâches** sont-elles attribuées aux différents services de votre organisation?
- Y-a-t-il une **personne responsable** pour chaque domaine d'activité?

(C)CeRFi SA - 2016

14



Données traitées

- Quels types de **dossiers/données** traitez-vous?
- De quelles **données personnelles** disposez-vous?

(C)CeRFI SA - 2016 15



Logiciels informatiques

- Quels **systèmes d'exploitation** utilisez-vous?
- Quelles **applications spécifiques** et **standards** utilisez-vous?

(C)CeRFI SA - 2016 16

Matériels informatiques

- Quelle est la **composition** globale de votre **parc informatique**?

- ordinateurs de bureau
- appareils mobiles
- imprimantes
- scanners
- etc.



(C)CeRFi SA - 2016

17



DROITS D'ACCÈS

(C)CeRFi SA - 2016

18

Droits d'accès

- Est-ce que chaque personne qui accède à votre système d'information a un **identifiant (login) unique**?
- Est-ce qu'un **collaborateur d'un service spécifique** peut accéder aux **données d'un autre service**?
- L'accès à votre système d'information est-il accordé à des **intervenants externes**?



(C)CeRFI SA - 2016

19

Droits d'accès

- ***"C'est notre fournisseur externe (société informatique) qui gère les droits d'accès à notre système d'information."***
- Il est fortement recommandé de ne pas laisser à un fournisseur externe la maîtrise des droits d'accès.
- **Les droits d'accès devraient toujours être gérés par les responsables des données (maîtres de fichiers).**

(C)CeRFI SA - 2016

20



(C)CeRFI SA - 2016

21

Droits d'accès



- A quels **types de données** accédez-vous?

Droits d'accès



- ***"Quasiment la moitié du personnel accède à des informations sensibles."***
- Une **gestion "fine" des droits d'accès**, ainsi que l'utilisation de **mots de passe "forts"**, doivent être mises en place.

(C)CeRFI SA - 2016

22



A stick figure character is sitting at a desk with a computer monitor, keyboard, and a mug. The character has its arms raised in a celebratory gesture, with motion lines above its head indicating excitement. The desk also has some papers and a small green box.

Droits d'accès ?

- Le **nombre de tentatives de connexion au système** est-il limité?

(C)CeRFI SA - 2016 23

Droits d'accès A

- ***"Le nombre de tentatives de connexion n'est pas limité."***
- Après **3 erreurs de connexion**, le système devrait bloquer l'accès, aussi bien sur les **appareils mobiles** que sur les **ordinateurs de bureau** (ou portables).

(C)CeRFI SA - 2016 24



MOTS DE PASSE

(C)CeRFi SA - 2016

25



Mots de passe

- Les mots de passe sont-ils **connus par d'autres personnes** que les utilisateurs eux-mêmes?

(C)CeRFi SA - 2016

26

A

Mots de passe (réponses)

- *"Les mots de passe de l'ensemble du personnel sont connus par la direction, et indirectement, par notre prestataire informatique."*
- *"La liste des mots de passe se trouve dans un dossier protégé sur notre serveur de fichiers."*

A

Mots de passe (recommandations)

- **Cette liste ne devrait pas exister**, car un mot de passe perd son caractère "personnel" à partir du moment où il est connu d'une tierce personne.
- Dans un premier temps, nous vous recommandons de mettre un **mot de passe "fort"** sur le fichier contenant tous les mots de passe de votre personnel.
- Dans un second temps, nous vous préconisons de **changer tous les mots de passe** et d'utiliser un **outil d'enregistrement des mots de passe**.
- **Avertissement**: si votre prestataire informatique peut se connecter à distance sur le poste de l'employé qui tient la liste des mots de passe, il accède aussi à la liste de tous les mots de passe du personnel.

Mots de passe

- La **syntaxe** des mots de passe est-elle importante pour vous?
- **Comment composez-vous votre mot-de-passe?**



(C)CeRFI SA - 2016

29

Mots de passe

- ***"La syntaxe de nos mots de passe nous imposée par notre administrateur."***
- Toute application informatique devrait exiger un mot de passe "fort" **d'au moins 8 caractères**, à changer **tous les 3 mois**.

m2U#6xQUN!cVQM8oDzPB!P

(C)CeRFI SA - 2016

30



(C)CeRFI SA - 2016

Verrouillage des appareils informatiques ?

- Les postes de travail sont-ils **verrouillés** en cas **d'absence du bureau**?

31

Verrouillage

- *"Oui, les postes de travail sont régulièrement verrouillés."*
- Il est très important que chaque personne possédant un appareil informatique le verrouille dès **qu'elle quitte son bureau**.



- **Remarque:** le verrouillage automatique n'est généralement pas suffisant, puisqu'il est souvent programmé à 10 ou 20 minutes.

(C)CeRFI SA - 2016

32




SUPPORTS DE DONNÉES

(C)CeRFi SA - 2016

33



Supports amovibles ?

- Enregistrez-vous des données sur des **supports amovibles**?
 - CD-ROM/DVD
 - clé USB
 - disque dur externe
 - Etc.

(C)CeRFi SA - 2016

34

Supports de données



- *"En principe non, il se peut cependant que des fichiers soient temporairement enregistrés sur des supports amovibles dans le contexte de présentations effectuées à l'extérieur."*
- Concernant vos supports de données amovibles, nous vous suggérons d'en tenir un **inventaire** et d'en définir les **règles d'utilisation**:
 - personnes autorisées à les utiliser
 - blocage des connecteurs USB sur la plupart des postes de travail, sauf sur ceux des personnes autorisées
 - procédure de contrôle des virus avant de les utiliser
 - procédure d'effacement de ces données après utilisation
- Si des supports amovibles sont utilisés pour transporter des données sensibles, ils devaient être **chiffrés**, même si les fichiers qu'ils contiennent sont protégés.




APPAREILS MOBILES



(C)CeRFI SA - 2016

37

Appareils mobiles

- Utilisez-vous des appareils portables?
- Vous arrive-t-il de transporter des **données confidentielles** sur ces appareils portables?
- Protégez-vous l'accès à ces appareils par un **mot de passe**?

Appareils mobiles

- *"Oui, la grande majorité de nos collaborateurs disposent d'un appareil mobile (smartphone et/ou tablette). Ces appareils sont protégés par un code PIN, mais pas par un mot de passe personnel".*
- Tout appareil portable qui contient des données personnelles ou qui permet de se connecter au SI de l'organisation, devrait être protégé, au minimum, par un **mot de passe personnel**.

(C)CeRFI SA - 2016

38

Appareils mobiles

- Pour vous faciliter la gestion de votre parc mobile, nous vous suggérons d'utiliser un outil de **MDM** permettant d'effectuer:
 - le blocage et l'effacement des données à distance (en cas de perte ou du vol)
 - l'installation de logiciels à travers le réseau cellulaire
 - la sauvegarde et la restauration des comptes des utilisateurs
 - etc.



LOCAUX, COURRIER POSTAL
ET FAX

Accès aux locaux

- Quelles sont les **mesures** particulières de **protection de vos locaux**?
- Les **clés** sont-elles **sécurisées** et **personnalisées**?
- Que se passe-t-il en cas de **vol de clés**?



(C)CeRFI SA - 2016

41

Accès aux locaux

- ***"La porte d'entrée principale est ouverte durant les heures de bureau."***
- **La porte d'entrée principale devrait être fermée 24 heures sur 24.**
- Pour faciliter les entrées et sorties, nous vous suggérons de faire poser un système de badge, plutôt que l'utilisation d'une clé supplémentaire.

(C)CeRFI SA - 2016

42

Courrier postal et fax

- **Comment le courrier interne est-il distribué?**
- Qu'en est-il du courrier avec une mention particulière?



(C)CeRFI SA - 2016

43

Courrier postal et fax

- ***"Nous utilisons le courrier postal, ainsi que le fax, comme modes d'expédition du courrier. C'est le secrétariat qui ouvre tout le courrier et qui le classe dans des casiers personnels, mais non fermés."***
- Idéalement, **les casiers devraient être fermés à clé**, d'autant plus qu'ils contiennent des données sensibles et que la porte principale d'accès aux bureaux n'est pas fermée à clé 24 heures sur 24.
- A court terme, **nous vous préconisons de déplacer votre fax ainsi que votre imprimante-scanner dans un bureau fermé à clé**, ou de tenir fermée la porte d'accès à vos locaux 24 heures sur 24.
- A l'avenir, nous vous préconisons:
 - soit d'équiper **chaque bureau** d'un fax ou d'une imprimante-scanner (qui peut aussi faire office de fax)
 - soit d'investir dans une **machine sécurisée**, qui permet, au moyen d'un code ou d'un badge, d'imprimer les documents uniquement lorsque la personne à laquelle ils sont destinés se trouvent devant l'appareil

(C)CeRFI SA - 2016

44



INTERNET

(C)CeRFi SA - 2016

45

Internet

- **Avez-vous un site Internet?**
- Ce site est-il **géré par un prestataire externe?**
- **Quel type de contrat** avez-vous avec ce prestataire?



(C)CeRFi SA - 2016

46

Internet



- *"La gestion de notre site Internet se fait en interne. Une seule personne en est responsable."*
- Il est de votre responsabilité de veiller à la bonne gestion de votre site Internet (qu'il soit géré en interne ou par un prestataire externe).
- Nous vous conseillons de vérifier les **accès au système de gestion de votre site Internet** en:
 - listant les **personnes** qui ont accès au système de mise à jour des pages (CMS) de votre site
 - vérifiant la composition des **mots de passe** utilisés
- **Attention:** si l'accès à un système informatique est partagé avec plusieurs personnes, il est impossible de savoir qui a fait quoi en cas de problème, voire même en cas de malveillance.
- Le même principe doit être appliqué sur un site interne (**Intranet**) ou sur un **réseau social**.



Messagerie électronique



- Echangez-vous des **données confidentielles** par courrier électronique?
- Quelles **précautions** appliquez-vous?
- Que faites-vous des **pièces jointes** que vous ne vous attendez pas à recevoir?

A

Messagerie électronique

- ***"Oui, nous échangeons de données confidentielles par courrier électronique, mais nous n'utilisons aucun système de protection spécifique."***
- Lors de la transmission de données par e-mail, il n'est pas possible d'exclure que le document parvienne à un autre destinataire que celui souhaité. Or, en tant qu'expéditeur, vous endossez la responsabilité de la transmission.
- **Nous vous suggérons d'éviter l'envoi d'informations confidentielles par e-mail avec des organismes externes.**
- **Nous vous conseillons soit de protéger les fichiers échangés (au moyen de "bons" mots de passe par exemple), soit de chiffrer les e-mails.**



RENSEIGNEMENTS DONNÉS
PAR TÉLÉPHONE



(C)CeRFI SA - 2016

Renseignements donnés par téléphone ?

- Donnez-vous des **renseignements confidentiels** par **téléphone**?
- Comment vous assurez-vous que les personnes auxquelles vous donnez des informations par téléphone sont **les "bonnes" personnes**?

51

Renseignements donnés par téléphone

- *"Ça peut arriver, mais pas sans les vérifications d'usages et uniquement aux personnes habilités à les recevoir."*
- Il est important de bien **authentifier** les personnes auxquelles vous donnez des renseignements confidentiels par téléphone pour vous prémunir de l'usurpation d'identité.
- Voici quelques conseils:
 - **rappelez vous-même votre interlocuteur** si vous ne le connaissez pas ou si vous avez le moindre doute
 - **demandez-lui un code**, une date de naissance ou toute autre information de ce type pour vous assurer de son identité

(C)CeRFI SA - 2016

52




SUPPORT INFORMATIQUE

(C)CeRFi SA - 2016

53

Support informatique

- Votre service de support informatique utilise-t-il une **application de connexion à distance**?
- A-t-il un **accès** qui lui est propre?
- Si ce service est assuré par un prestataire externe, lui avez-vous fait signer une **clause de confidentialité**?



(C)CeRFi SA - 2016

54

Support informatique

A

- *"L'application de connexion à distance utilisée par notre prestataire informatique est TeamViewer."*
- L'accès à distance devrait se faire au moyen d'un mot de passe "temporaire" et être remis (par téléphone) par l'utilisateur à la personne qui veut "prendre la main" sur son ordinateur.
- Or, il arrive que votre prestataire informatique se connecte sur le poste d'un utilisateur **sans lui demander le mot de passe "temporaire" de TeamViewer.**

Maintenance informatique

A

- *"Les intervenants externes utilisent quelque fois les accès des employés - qui le leur donnent."*
- **Personne ne devrait JAMAIS utiliser l'accès d'une autre personne.** Chaque accès doit être individuel.
- Il est donc très important que les intervenants externes aient **leurs propres accès** (login, mot de passe) pour leurs interventions sur votre système informatique.

Support informatique

A

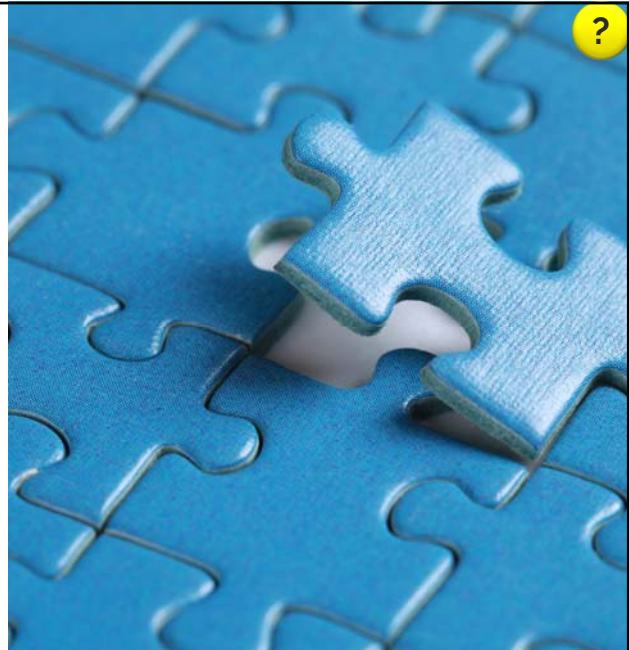
- ***"Nous devons vérifier si une clause de confidentialité existe."***
- Nous vous suggérons de vérifier si une **clause de confidentialité** figure dans les contrats de support ou de maintenance établis par vos partenaires en informatique.
- Quel que soit le prestataire externe auquel vous confiez la gestion de votre système d'information, **vous en gardez la responsabilité.**



RÈGLEMENT D'UTILISATION DU SYSTÈME D'INFORMATION

Règlement d'utilisation du système d'information

- Disposez-vous d'un **règlement d'utilisation de votre système d'information**?
- Ce règlement est-il **connu** de l'ensemble du personnel?



(C)CeRFI SA - 2016

59



(C)CeRFI SA - 2016

Sensibilisation à la sécurité

- Le personnel de l'organisation a-t-il suivi une **sensibilisation à la sécurité de l'information**?

60

B

Sensibilisation à la sécurité

- *"Nous ne disposons pas de règlement d'utilisation de notre système d'information.*
- *Notre personnel n'a jamais vraiment suivi de formation à la sécurité informatique. Tout au plus, chaque nouveau collaborateur est "informé" à son arrivée dans l'entreprise."*

B

Règlement d'utilisation du système d'information et sensibilisation à la sécurité

- Nous vous suggérons de mettre en place un règlement d'utilisation de votre système d'information dans son ensemble:
 - traitement des **données personnelles** et **sensibles**
 - utilisation du **matériel**
 - utilisation **d'Internet**, des **réseaux sociaux** et de la **messagerie électronique**
 - utilisation du **téléphone**
 - gestion des **tiers**
 - **vidéosurveillance**
 - accès aux **locaux**
 - **entrées et sorties du personnel**
 - **dispositifs de contrôles**
 - etc.





DÉPLACEMENTS PROFESSIONNELS

(C)CeRFi SA - 2016

63

Déplacements professionnels

- Comment effectuez-vous vos **déplacements professionnels**?
- Comment protégez-vous les **dossiers** que vous transportez?
- Avec quels types de matériel informatique vous déplacez-vous?



(C)CeRFi SA - 2016

64



Déplacements professionnels

- *"Nous effectuons nos déplacements principalement en voiture privée."*
- Nous préconisons de transporter les dossiers "sensibles" dans une **mallette sécurisée**, de ne jamais les laisser dans un **véhicule** en stationnement et de ne pas les ouvrir dans un **lieu public**.



PERSONNEL EXTERNE

Personnel externe

- Faites-vous appel à des **collaborateurs externes**?
- Les **stagiaires** sont-ils considérés comme des collaborateurs internes ou externes?



(C)CeRFI SA - 2016

67



(C)CeRFI SA - 2016

Personnel externe

- Chaque collaborateur externe dispose-t-il d'une **place de travail** au sein de votre organisation, ainsi que d'un **accès au système d'information**?

68

B

Personnel externe

- Voir **proposition sur la clause de confidentialité.**
- Voir aussi **proposition sur le règlement d'utilisation du système d'information.**



ARCHIVAGE



(C)CeRFI SA - 2016

Archivage



- Avez-vous une **procédure de destruction de vos archives?**

71

Archivage



- ***"Non, nous n'avons aucune procédure sur la destruction de nos archives. Nous gardons tout."***
- Nous vous préconisons de mettre en place une **procédure de destruction des archives** (incinération).
- De plus, le lieu d'archivage des documents n'étant pas protégé contre les inondations, nous vous suggérons au moins de **surélever** les documents à 20 ou 30 cm du sol.

(C)CeRFI SA - 2016

72

**Avez-vous des
questions?**



**Merci beaucoup
de votre attention**

