

Thème 1 Chapitre 2

Appliquer et diffuser la réglementation liée aux données à caractère personnel

TP 1

Concevoir une journée de formation sur la protection des données à caractère personnel

Bloc 3 - Cybersécurité des services informatiques

EVALUATION DES COMPETENCES VISEES						
Compétence(s) Visée(s)	Savoir-Faire(s)	Niveau d'acquisition				
		A	B	C	D	E
B3.1 : Protéger des données à caractère personnel	Identifier les risques liés à la collecte, au traitement, au stockage					
	Sensibiliser les utilisateurs à la protection des données à caractère personnel					

Mission

Chaque utilisateur du système d'information est un maillon d'une chaîne : la défaillance de l'un d'entre eux compromet toute la chaîne. D'où l'importance de tous les sensibiliser à la protection des données à caractère personnel. Ainsi, CentreCall met en place une journée de formation destinée aux nouveaux opérateurs téléphoniques.

Cette formation est organisée en deux ateliers : la sensibilisation à la protection des données à caractère personnel (atelier 1) et la présentation de la politique de protection des données personnelles de CentreCall (atelier 2).

Vous êtes en charge de la conception de cette session de formation et de l'élaboration de supports adaptés aux stagiaires.

Table des matières

Mission	1
ÉTAPE 1 : Préparation du protocole de la formation.....	3
1 - Préparation du protocole de la formation	3
ÉTAPE 2 : Préparation des supports de l'atelier 1	3
2 - Test du scénario d'immersion des opérateurs téléphoniques	3
ÉTAPE 3 : Préparation des supports de l'atelier 2	10
3 - Diaporama sur politique de protection des données à caractère personnel	10
ÉTAPE 4 : Évaluation et suivi de la formation.....	10
4 - Choix d'un outil d'évaluation et vérification des acquis.....	10
Document 1	11
Document 2	11
Document 3 – Schéma réseau	11
Document 6	13
Document 1 – Mission 1	13

ÉTAPE 1 : Préparation du protocole de la formation

1 - Préparation du protocole de la formation

1.1 - Objectif principal de la formation et objectifs intermédiaires

Définissez l'objectif principal de la formation et les objectifs intermédiaires, à partir du programme de la journée.

Documents 1 et 2

1.2 - Approche pédagogique pour chaque atelier

Choisissez l'approche pédagogique la plus appropriée à chaque atelier. Justifiez.

ÉTAPE 2 : Préparation des supports de l'atelier 1

Pour faciliter l'écoute des nouveaux opérateurs téléphoniques, un scénario d'immersion a été imaginé. Pour la mise en œuvre du scénario proposé, vous devrez utiliser plusieurs machines :

- **VM votrelogin_T_rocky9_mariadb_apache_phpmyadmin_1A_TC3** qui héberge un serveur de base de données (mariadb), un serveur web (Apache) et une application web (phpmyadmin)
Pour les tests, vous devrez mettre en place la base de données **dbcallmanager** et créer plusieurs utilisateurs avec certains privilèges sur cette base.
- **VM Windows 10** qui servira de client pour le call manager
- **Votre poste de travail** (machine Fedora) qui servira de client pour l'opérateur téléphonique

Le schéma réseau de cette petite infrastructure est donné dans le Document 3

2 - Test du scénario d'immersion des opérateurs téléphoniques

Testez le scénario d'immersion des opérateurs téléphoniques en respectant le cahier des charges présenté dans le document 3

2.1 - Configuration du serveur de base de données (VM rocky9 dans Vmware)

Compte utilisateur : btssio / btssio

Compte administrateur : root / joliverie

Renommage de la machine

- Démarrez votre VM rocky9 et renommez le nom de machine (pas celui dans Vmware)
 - Nom de la forme : **rocky9-PNNNN.jolsio.net** (ex : rocky9-**BMORA**.jolsio.net pour **Bob MORANE**)

Sélection du VLAN

- Sélectionnez le VLAN **SIO - PEDAGO**

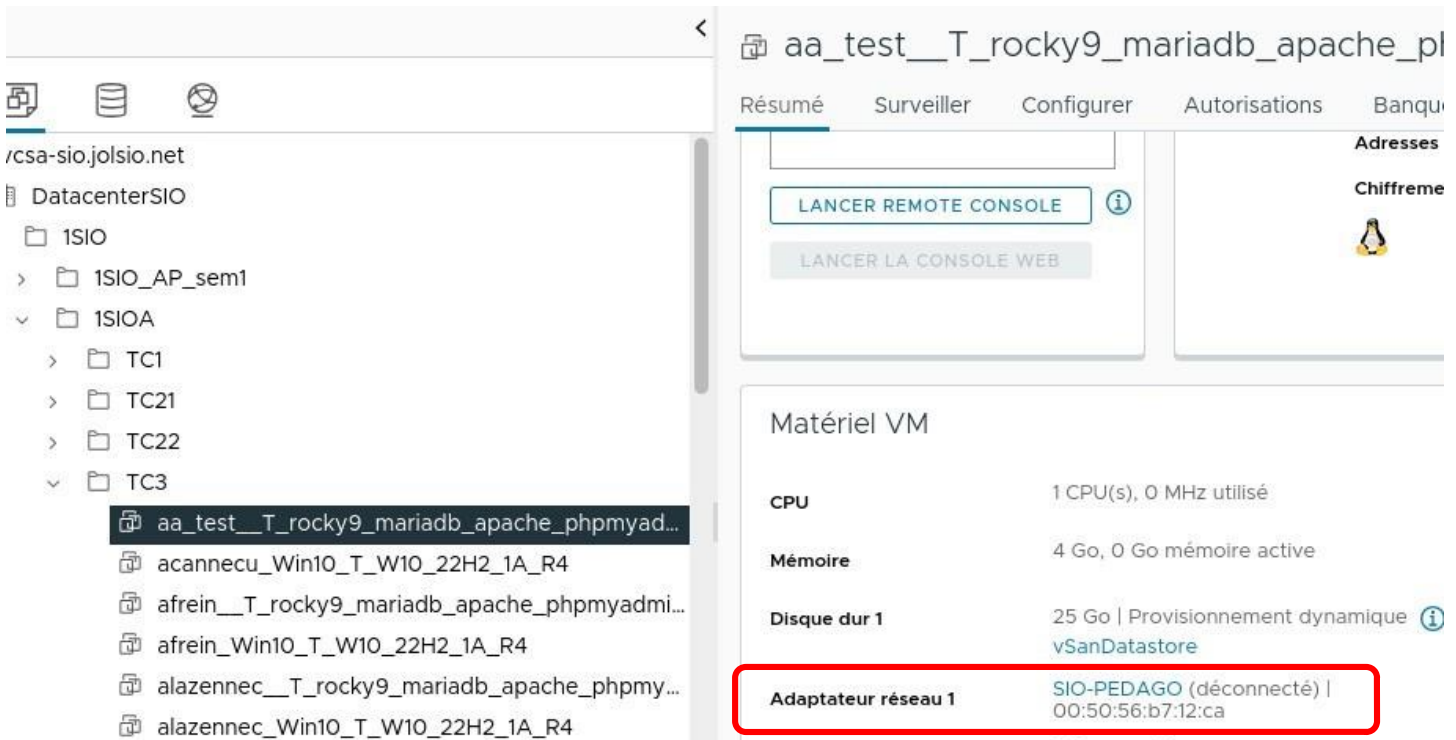


Figure 1: Exemple de sélection de VLAN (ici, SIO-PEDAGO)

Vérification paramètre réseau

- Notez l'adresse IP qui vous a été attribuée à l'aide d'un terminal avec la commande **ip a** (ou **ip -c a**). Regardez l'interface **ens192** (ou quelque chose qui ressemble).

```
[btssio@centos8 ~]$ ip -c a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens192: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 00:50:56:b7:0c:a2 brd ff:ff:ff:ff:ff:ff
    inet 10.15.12.35/22 brd 10.15.15.255 scope global dynamic noprefixroute ens192
        valid_lft 2742sec preferred_lft 2742sec
    inet6 fe80::ce65:3aef:bb9f:2fc8/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
3: virbr0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether 52:54:00:de:7b:d2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.122.1/24 brd 192.168.122.255 scope global virbr0
        valid_lft forever preferred_lft forever
4: virbr0-nic: <BROADCAST,MULTICAST> mtu 1500 qdisc fq_codel master virbr0 state DOWN group default qlen 1000
    link/ether 52:54:00:de:7b:d2 brd ff:ff:ff:ff:ff:ff
```

Figure 2: Dans cette capture d'écran, l'adresse IP est **10.15.12.35**

2.2 - Vérification du bon fonctionnement des services du serveur rocky

- Vérifiez que le service de base de données (**mariadb**) est bien actif

commande : **\$ systemctl status mariadb**

```
[btssio@centos8 ~]$ systemctl status mariadb
● mariadb.service - MariaDB 10.3 database server
   Loaded: loaded (/usr/lib/systemd/system/mariadb.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-10-03 12:14:41 EDT; 30min ago
```

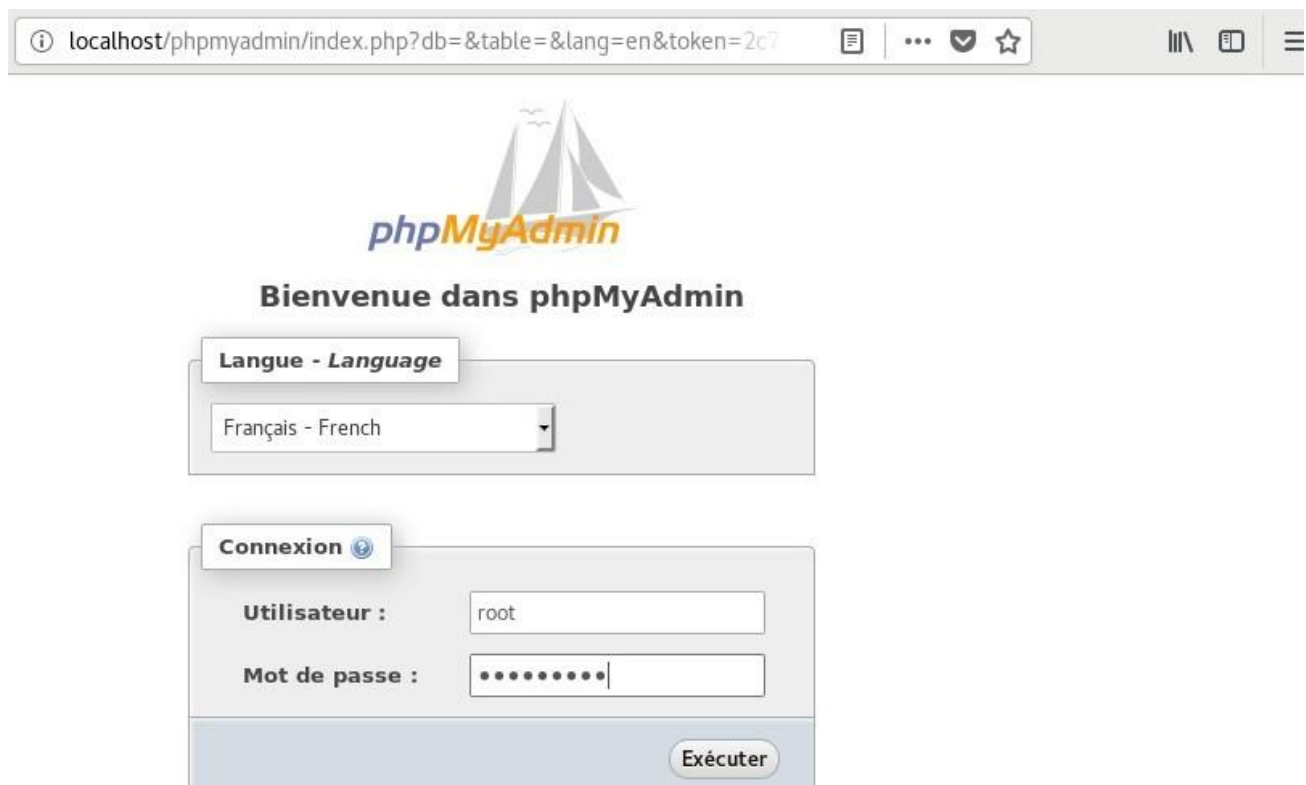
- Vérifiez que le service du serveur web (**httpd**) est bien actif commande : **\$ systemctl status httpd**

```
[btssio@centos8 ~]$ systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; enabled; vendor preset: disabled)
  Drop-In: /usr/lib/systemd/system/httpd.service.d
           └─php-fpm.conf
   Active: active (running) since Mon 2022-10-03 12:14:40 EDT; 31min ago
```

Vérifiez que l'application Web **phpmyadmin** est bien opérationnelle

Compte administrateur : **root / joliverie**

<http://localhost/phpmyadmin>



Vérifiez que les ports des services mariadb et httpd sont bien ouverts commande : **\$ ss -antup | grep LISTEN** (httpd : port 80, mariadb : port 3306)

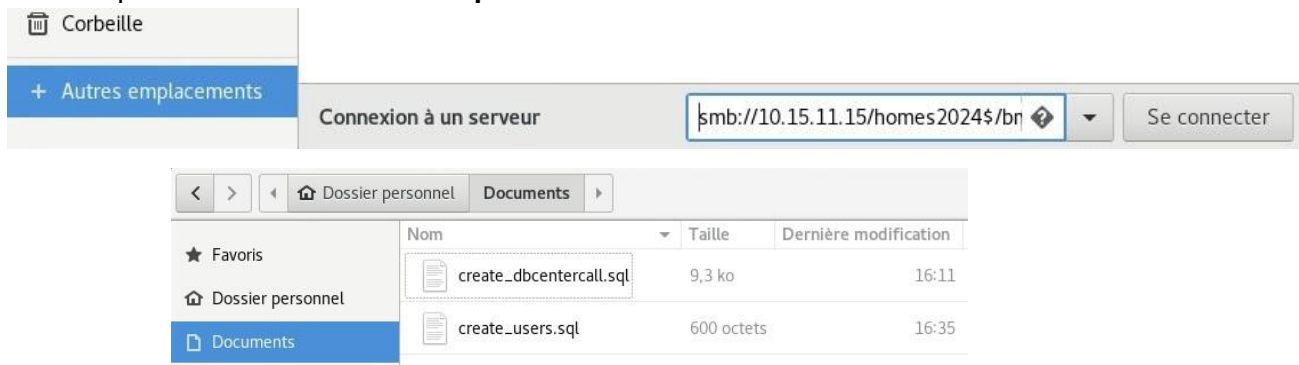
```
[btssio@centos8 ~]$ ss -antup | grep LISTEN
tcp LISTEN 0      32      192.168.122.1:53      0.0.0.0:*
tcp LISTEN 0      128     0.0.0.0:22      0.0.0.0:*
tcp LISTEN 0      5       127.0.0.1:631     0.0.0.0:*
tcp LISTEN 0      80      0.0.0.0:3306     0.0.0.0:*
tcp LISTEN 0      128     0.0.0.0:111     0.0.0.0:*
tcp LISTEN 0      128     [::]:22        [::]:*
tcp LISTEN 0      5       [::1]:631      [::]:*
tcp LISTEN 0      128     [::]:111       [::]:*
tcp LISTEN 0      128     *:80           *:*
```

2.3 - Mise en place de la base de données et des utilisateurs

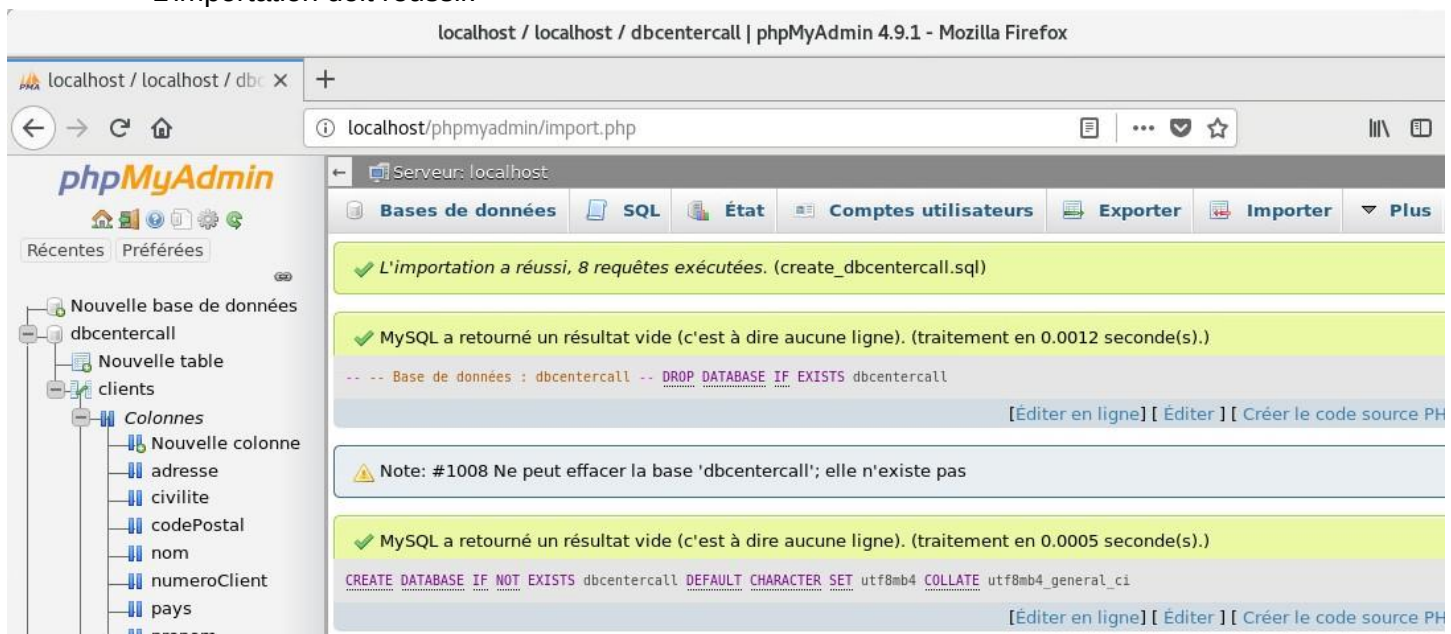
Dans cette partie, nous allons créer la base de données **dbcentercall** dans le SGBD MariaDB à partir du fichier **create_dbcentercall.sql**. Ensuite, nous allons créer 3 utilisateurs avec différents privilèges sur cette bdd à partir du fichier **create_users.sql**.

- Téléchargez les scripts **create_dbcentercall.sql** et **create_users.sql** à partir de Moodle
- Copiez ces fichiers dans votre serveur en utilisant un partage réseau (dans par exemple : **/home/Documents**)
Mettez en place un lecteur réseau dans votre serveur pointant sur votre espace de stockage personnel. Gestionnaire de fichiers du serveur – Autres emplacement
smb://10.15.11.2/homes2024\$/votrelogin

Copiez ensuite les fichiers **.sql** dans votre serveur



- Importez la base de données **dbcallmanager** dans **mariadb**
 - Lancez **phpmyadmin** et authentifiez-vous avec le compte administrateur **root**
 - Cliquez l'onglet **Importer** dans la page d'accueil puis sélectionner le fichier **create_dbcentercall.sql** ... **Exécuter**
L'importation doit réussir.



- Vérifiez la présence de la bdd **dbcentercall** et de ses tables
- Importez les utilisateurs de cette bdd avec leurs privilèges
 - Cliquez l'onglet **Importer** dans la page d'accueil puis sélectionner le fichier **create_users.sql** ... **Exécuter**. L'importation doit réussir.

Vérifiez la présence des nouveaux utilisateurs créés

- Cliquez l'onglet **Comptes utilisateurs** dans la page d'accueil

Nom d'utilisateur	Nom d'hôte	Mot de passe	Privilèges globaux	Groupe d'utilisateurs	« Grant »	Action
<input type="checkbox"/> calladmin1	localhost	Oui	USAGE		Non	Éditer les privilèges
<input type="checkbox"/> callman1	%	Oui	USAGE		Non	Éditer les privilèges
<input type="checkbox"/> opera1	%	Oui	USAGE		Non	Éditer les privilèges
<input type="checkbox"/> root	127.0.0.1	Oui	ALL PRIVILEGES		Oui	Éditer les privilèges
<input type="checkbox"/> root	::1	Oui	ALL PRIVILEGES		Oui	Éditer les privilèges
<input type="checkbox"/> root	localhost	Oui	ALL PRIVILEGES		Oui	Éditer les privilèges

Figure 3: Les 3 nouveaux utilisateurs **calladmin1**, **callman1** et **opera1** viennent d'être créés

2.4 - Test de communication avec les 2 autres machines

- Récupérez les adresses IP de votre station de travail et de votre VM Windows 10. Notez-les.
- Testez la communication entre votre station de travail et le serveur. Cela doit fonctionner.
commande : **ping adresse_IP_destination** (à faire dans les 2 sens) **CTRL C** pour stopper

```
[tux@ordihd-fd35 ~]$ ping 10.15.12.35
PING 10.15.12.35 (10.15.12.35) 56(84) octets de données.
64 octets de 10.15.12.35 : icmp_seq=1 ttl=63 temps=129 ms
64 octets de 10.15.12.35 : icmp_seq=2 ttl=63 temps=135 ms
64 octets de 10.15.12.35 : icmp_seq=3 ttl=63 temps=155 ms
```

Figure 4: Exemple de test de communication entre la station Fedora et le serveur. Prenez VOTRE adresse IP de serveur et non celle donnée dans cette capture d'écran.

```
[btssio@centos8 ~]$ ping 10.1.201.6
PING 10.1.201.6 (10.1.201.6) 56(84) bytes of data.
64 bytes from 10.1.201.6: icmp_seq=1 ttl=63 time=69.8 ms
64 bytes from 10.1.201.6: icmp_seq=2 ttl=63 time=44.1 ms
64 bytes from 10.1.201.6: icmp_seq=3 ttl=63 time=34.1 ms
```

Figure 5: Exemple de test de communication entre la station Fedora et le serveur (test dans l'autre sens). Prenez VOTRE adresse IP de station Fedora et non celle donnée dans cette capture d'écran. Ici, le test est fait avec une station connectée au LAN par VPN (adresse en 10.1.X.Y).

Si cela ne fonctionne pas :

- vérifiez que les 2 machines sont dans le même VLAN (SIO-PEDAGO)
- vérifiez que les 2 adresses IP ont la même adresse de réseau
- vérifiez que le pare-feu est bien désactivé sur la machine cliente dans le cas d'une machine Windows
- Testez la communication entre votre VM Windows 10 et le serveur, dans les 2 sens. Cela doit fonctionner.

Testez l'accès au serveur de base de données à partir de la machine cliente Fedora
http://adresse_IP_serveurBDD/phpmyadmin



Figure 6: Accès au serveur de base de données à partir de la machine cliente Fedora

Testez l'accès au serveur de base de donnVoir Document 3ées à partir de la VM Windows 10

2.5 - Mise en œuvre du scénario

Voir Document 3

Réalisez chaque étape du scénario. Résumez dans un tableau récapitulatif les actions possibles ou non par compte utilisateur. Faites quelques captures d'écran pour chacune des étapes.

	Opérateur téléphonique opera1	Call manager calman1	Administrateur calladmin1
Consulter les données de la bdd	X	X	X
Modifier les données d'un champ d'une table			
Supprimer un enregistrement d'une table			
Créer une table			
Supprimer une table de la base de données			
Exécuter un script de création de bdd avec ses données			



Figure 7: Exemple : Les call managers n'ont pas le droit de créer de table

Qui sera responsable de la suppression des données personnelles aux yeux de l'équipe de sécurité du réseau ?

- Concluez sur l'importance de la mise en place des habilitations en fonction du poste occupé dans l'entreprise et de l'importance de sensibiliser le personnel à la protection des données à caractère personnel.

2.6 - Critique du support de sensibilisation

Critiquez le support de sensibilisation présenté dans le document 4, puis réalisez votre propre version en utilisant un logiciel adapté (par exemple canva.com). Le document sera au format d'une feuille A4.

ÉTAPE 3 : Préparation des supports de l'atelier 2

3 - Diaporama sur politique de protection des données à caractère personnel

Élaborez un diaporama présentant les points essentiels de la politique de protection des données à caractère personnel de CentreCall.

Reprenez les principaux éléments du contexte de CentreCall pour concevoir votre proposition de diaporama (Document 1 mission 1 ch2 , Document 1 mission 2 ch2).

Pour optimiser la présentation du diaporama, il existe des préconisations à respecter :

« L'objectif est d'insérer un minimum de texte. Pour que le diaporama reste un support visuel, chaque diapositive doit comporter au maximum trente mots, soit trois à quatre phrases. Le message doit être clair, simple et lisible.

Guy Kawasaki préconise, dans son ouvrage *L'art de se lancer*, la règle des « 10/20/30 » :

- 10 pour le nombre de diapos de façon à rester concis ;
- 20 pour les 20 minutes que doit durer une présentation, avant que l'intérêt de l'auditoire ne faiblisse ;
- 30 pour le corps de la police à utiliser dans une diapo.

La réflexion sur le design et la composition graphique que l'on souhaite appliquer à la présentation intervient au début et non à la fin. Elle dépend des idées à véhiculer, à organiser, à clarifier : • disposition : contraste, sens de la lecture, hiérarchie, position ;

- éléments visuels : fond, couleur, texte, image.

Par ailleurs, il est recommandé de laisser 50 % de la diapositive vierge : cela permet de mettre en relief davantage les informations et images affichées.

Pour choisir la couleur à utiliser dans la diapositive ou des éléments, il faut prendre en compte la charte graphique ou les couleurs du logo de l'entreprise.

Il est fortement recommandé :

- de ne pas utiliser plus de deux polices différentes ;
- homogénéiser la taille de police d'une diapositive à l'autre, sauf pour différencier volontairement un message par rapport à un autre.

L'image a une triple fonction, c'est pour cela qu'il faut faire attention à la netteté et la clarté de l'image :

- illustrer efficacement le propos ;
- favoriser la mémorisation du message ;
- libérer l'orateur de son écran. »

Source : https://fr.wikiversity.org/wiki/Diaporamas/Règles_d'utilisation

ÉTAPE 4 : Évaluation et suivi de la formation

4 - Choix d'un outil d'évaluation et vérification des acquis

Choisissez un outil d'évaluation adapté et listez cinq questions qui pourraient être posées en fin d'intervention pour vérifier les acquis des nouveaux opérateurs téléphoniques.

Document 1**Organisation de La journée de formation**

8h00 - 9h00	Accueil des nouveaux opérateurs téléphoniques.
9h00 - 12h00	Atelier 1. Sensibilisation à la protection des données à caractère personnel.
14h00 - 17h00	Atelier 2. Présentation de la politique de protection des données personnelles de CentreCall.
17h00 - 17h30	Évaluation de la formation.

Document 2**Processus de préparation d'une session de formation****Définition des objectifs de la formation**

Les objectifs de la formation doivent être clairement identifiés avant l'intervention, afin de faciliter la cohérence entre le message diffusé, les supports mobilisés et l'évaluation des acquis. Un cahier des charges de la formation, comprenant les messages à véhiculer et le déroulé de la formation, doit être rédigé avant l'intervention.

Prise en compte des « qualités des apprenants »

La « qualité des apprenants » revêt deux dimensions : leur personnalité et leurs prérequis quant au sujet de la formation. Le formateur doit en tenir compte pour ne pas se retrouver décalage avec son public.

La personnalité peut être appréhendée pendant les premiers moments de l'intervention, afin d'adapter son discours.

Les prérequis doivent être analysés en amont de l'intervention par un diagnostic du niveau de connaissance des apprenants sur le sujet à traiter.

Adaptation de l'approche pédagogique au public visé

L'étape précédente doit aider le formateur à adopter une position face à son public. Plusieurs approches peuvent être mobilisées, dont les deux suivantes :

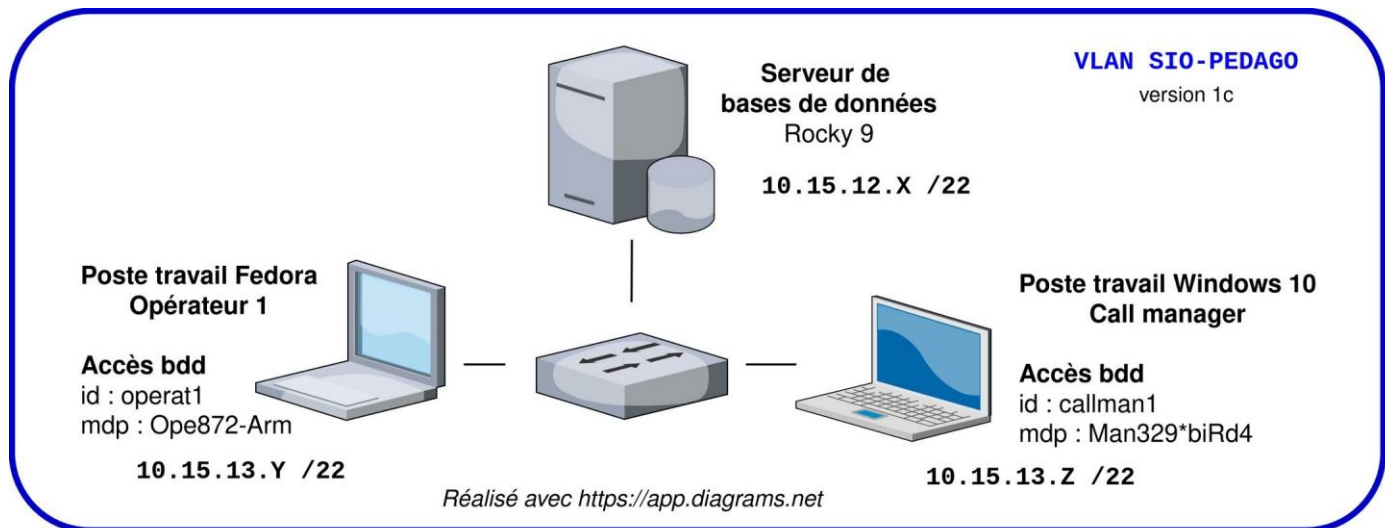
Approche démonstrative	Approche participative
<p>Le formateur transmet un message aux apprenants par une démonstration claire qui doit être, si possible, appuyée d'illustrations.</p> <p>Cette méthode peut être utilisée si le formateur a besoin de donner des informations sans avoir à soulever de problématique.</p> <p><i>Exemple : présentation par le formateur des règles à appliquer pour l'authentification des utilisateurs.</i></p>	<p>Les apprenants réalisent des travaux ou répondent à un questionnement qui va permettre de construire collectivement le message à intégrer.</p> <p>Cette méthode facilite la compréhension, car l'apprenant est acteur de sa formation.</p> <p>Exemple : un exercice guidé par des questions sur les vulnérabilités d'une application.</p>

Document 3 – Schéma réseau**Cahier des charges de l'atelier 1 : scénario d'immersion pour la sensibilisation à la protection des données à caractère personnel****Définition des objectifs de la formation**

L'atelier doit attirer l'attention des stagiaires sur l'importance d'être vigilant à l'égard de la protection des données à caractère personnel et les aider à adapter leur comportement.

Dans cet objectif, il a été convenu de préparer un scénario d'immersion pour la sensibilisation à la protection des données à caractère personnel.

Schéma réseau



Remarque : les valeurs des adresses IP sont données à titre indicatif. A vous d'obtenir les valeurs correspondant à votre environnement.

Comptes utilisateurs de Centercall permettant d'accéder à la base de données dbcentercall

Utilisateur	Identifiant	Mot de passe
Opérateur téléphonique	opera1	Ope872-Arm
Call Manager	callman1	Man329*biRd4
Administrateur Centercall	calladmin1	Adm!734+AlF1

Mise en œuvre du scénario

1. L'opérateur téléphonique 1 se connecte à la base de données à partir de la machine Fedora et consulte la liste des clients contenue dans la base de données.
2. L'opérateur téléphonique 1 s'absente quelques instants en laissant sa session ouverte. Un collègue, qui s'est fâché récemment avec cet opérateur téléphonique, essaie de modifier les données d'un client. Puis il essaie d'en supprimer un autre, et de supprimer la table clients. Il essaie enfin de supprimer toute la base de données.
3. Le Call manager 1 se connecte à la base de données à partir de la VM Windows 10. Il consulte la liste des clients contenue dans la base de données. Il essaie de modifier les données d'un client puis essaie d'en supprimer un autre.
4. Le Call Manager 1 part faire une pause et laisse sa session ouverte. L'opérateur téléphonique 1, passant par là, utilise l'ordinateur du Call manager laissé libre. Il profite de la session restée ouverte pour réaliser des consultations de la table « clients ». Malheureusement, il fait une erreur de manipulation et supprime le contenu de la table. Effrayé par la gravité de son erreur et ses conséquences, il décide de ne rien dire.
5. Le Call Manager 1 se rend compte plus tard que la table clients a été supprimée. Il panique et essaie de supprimer la base de données **dbcentercall**. Il essaie ensuite d'exécuter le script **create_dbcentercall.sql** qu'il a réussi à récupérer.
6. L'administrateur de Centercall se rend compte que les données de la base de données ont été modifiées. Il le signale au responsable de Centercall qui lui demande de supprimer la base de données et de restaurer la version la plus récente. Il essaie d'effectuer ces opérations à partir de la machine cliente Fedora, puis à partir du serveur de base de données.

Document 4**Support de sensibilisation au respect de la confidentialité des données**

Il est décidé de sensibiliser les opérateurs téléphoniques et les call managers à la nécessité de ne pas laisser leur session de travail ouverte lorsqu'ils quittent leur poste. Cette affiche sera visible dans toutes les salles informatiques de l'entreprise :

Il est rappelé à l'ensemble des utilisateurs qu'il faut fermer votre session de travail avant de quitter votre poste afin de respecter la confidentialité des données.

L'équipe de la DSI





Document 5**Cahier des charges de l'atelier 2 : présentation de la politique de protection des données à caractère personnel de CentreCall**

L'atelier doit permettre de présenter la politique de protection des données à caractère personnel de CentreCall. Il comprend l'information à destination des utilisateurs du site vitrine de l'entreprise, mais aussi les éléments de la charte informatique de CentreCall.

Ces informations sont inconnues des nouveaux opérateurs téléphoniques.

Document 6**Outils de présentation et d'évaluation**

Voici quelques exemples d'outils de présentation ou d'évaluation (en accès gratuit) qui peuvent être utilisés lors d'une journée de formation.

Outils de présentation	Outils d'évaluation
 Prezi Prezi est le concurrent de PowerPoint le plus connu aujourd'hui. Il permet de dynamiser les présentations avec de nombreux effets.	 Plickers est une application en ligne permettant de générer des QCM interactifs.
 LibreOffice The Document Foundation La solution <i>open source</i> LibreOffice propose un logiciel de présentation dont l'interface est très similaire aux anciennes versions de PowerPoint.	 Kahoot est un système de quizz en ligne, simple à utiliser et stimulant pour les participants. Il offre un état clair, sous format Excel, de ce que les apprenants ont retenu.

Document 1 – Mission 1**Extrait de la charte de confidentialité publiée sur le site de CentreCall**

La publication de notre politique de confidentialité vous informe des finalités des traitements réalisés sur les données que vous nous communiquez.

CentreCall s'engage à assurer le meilleur niveau de protection de vos données personnelles, en conformité avec les réglementations européennes et françaises en vigueur.

CentreCall utilise vos données personnelles pour les finalités suivantes

- **La réalisation d'études de marché pour le compte de nos clients**

Nous recueillons les informations suivantes pour la réalisation des études de marché : vos coordonnées, vos motivations pour l'achat d'un produit ou d'un service.

- **L'externalisation de l'accueil téléphonique de nos clients**

Les appels téléphoniques reçus ou émis pour le compte de clients peuvent faire l'objet d'enregistrements audio.

- **La sécurité de notre site**

Nous collectons certaines données de navigation afin d'assurer la sécurité de nos services et de détecter, éviter ou retracer toute tentative de malveillance, intrusion informatique ou violation des conditions d'utilisation de ces services.

- **La personnalisation des publicités en ligne**

Nous pouvons utiliser des données qui ne permettent pas de vous identifier directement (identifiants techniques ou données sociodémographiques) afin d'adapter la publicité que vous visualisez sur notre site ou sur ceux de nos partenaires. Vos données peuvent être croisées avec d'autres données de navigation collectées à l'occasion de nos relations avec des partenaires. Pour plus d'informations et le suivi de vos **cookies**, rendez-vous à la page «cookies» du site.

Quelles sont les données personnelles collectées ?

Du fait de vos échanges avec nos opérateurs téléphoniques ou de votre inscription sur notre site, nous collectons et traitons les données suivantes : vos nom, prénom, adresse, adresse courriel, mot de passe, numéro de téléphone, préférences et centres d'intérêts, enregistrements de conversation. **Comment est assurée la sécurité des données personnelles ?**

La protection de la confidentialité et de **l'intégrité** de l'ensemble des données à caractère personnel collectées par notre organisation est assurée par la mise en place de plusieurs dispositifs :

un pare-feu certifié **ANSSI** assure le filtrage et la détection des tentatives d'intrusions ; l'ensemble de nos serveurs de données sont répliqués pour permettre, en cas de perte de données, une restauration sécurisée et rapide; les applications développées par nos services pour collecter et traiter les données à caractère personnel intègrent des solutions qui sécurisent les flux d'informations et évitent des actes malveillants.

Document 1 – mission 2

Extrait de projet de charte informatique

RÈGLES DE PROTECTION DES DONNÉES PERSONNELLES

1. Domaine d'application de la charte

Les règles décrites dans la présente charte s'appliquent à tout le personnel utilisant les moyens informatiques de CentreCall, ainsi que tout autre moyen de connexion à distance, afin d'accéder via Internet à tout service ou traitement électronique interne ou externe de l'entreprise, y compris l'accès à Internet.

Le non-respect d'une de ces règles est susceptible d'entraîner des mesures disciplinaires internes voire, en cas de violation d'un texte législatif ou réglementaire, des poursuites judiciaires. Les diverses lois concernant ce domaine sont présumées connues.

2. Conditions d'accès de l'utilisateur

- L'utilisation des ressources informatiques de l'entreprise est soumise à autorisation préalable.
- Cette autorisation est concrétisée par l'ouverture d'un compte utilisateur (création d'un courriel et d'un identifiant pour l'accès au réseau de l'entreprise).
- Cette autorisation est strictement personnelle et ne doit en aucun cas être cédée, même temporairement, à un tiers.

- Cette autorisation ne vaut que pour les activités conformes aux missions de l'entreprise, dans le respect de la législation en vigueur.
- L'entreprise se réserve le droit de retirer à tout moment cette autorisation et ce, sans préavis.
- Chaque utilisateur doit user raisonnablement des ressources partagées auxquelles il accède.
- L'usage de ces ressources est, pour l'essentiel, dédié à des utilisations professionnelles.
- L'usage personnel doit rester limité.

3. Respect de la confidentialité des informations

- Les utilisateurs ne doivent pas tenter de lire, copier, divulguer ou modifier les fichiers d'un autre utilisateur sans y avoir été autorisés.
- Les utilisateurs doivent s'interdire toute tentative d'interception de communications entre tiers.
- Les utilisateurs sont tenus à la réserve d'usage sur toute information relative au fonctionnement interne de l'entreprise.
- Les utilisateurs sont tenus de prendre, avec l'aide éventuelle du service informatique et du BPO (Data Protection Officer, délégué à la protection des données), les mesures de protection des données nécessaires au respect des engagements de confidentialité pris par l'entreprise vis-à-vis de tiers.
- Une attention toute particulière doit être portée à la confidentialité des bases de données CentreCall. Leur utilisation doit respecter les engagements de CentreCall.