AUTORITÉ DE PROTECTION DES DONNÉES PERSONNELLES
(APDP)

FORMATION DES DÉLÉGUÉS À LA PROTECTION DES DONNÉES PERSONNELLES

Thème : Audit et outils de gestion des risques relatifs aux données personnelles

Intervenant : Emmanuel ZOSSOU

Décembre 2021

Sommaire

INTRODUCTION

- La gestion des risques permet de déterminer les précautions à prendre « au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».

- En effet, la sécurité du système d'information d'une entreprise est un requis important pour la poursuite de ses activités. Qu'il s'agisse de la dégradation de son image de marque, du vol de ses secrets de fabrication ou de la perte de ses données clients ; ***une catastrophe informatique a toujours des conséquences fâcheuses pouvant aller jusqu'au dépôt de bilan.***

- Organiser cette sécurité n'est pas chose facile, c'est pourquoi il existe des méthodes reconnues pour aider les responsables de traitement à mettre en place une bonne politique de sécurité et à procéder aux audits permettant d'en vérifier l'efficacité.

I. Normes de sécurité : les méthodes d'analyse des risques

A. Politique de sécurité
B. Audit
C. Tableau comparatif des normes
D. Présentation des principales normes
E. Critères de choix

I. Normes de sécurité : les méthodes d'analyse des risques

A. Politique de sécurité

- **Une politique de sécurité** peut être vue comme l'ensemble des modèles d'organisation, des procédures et des bonnes pratiques techniques permettant d'assurer la sécurité du système d'information.
- **Mais qu'est-ce que la sécurité d'un SI** ? Elle tourne autour des 5 principaux concepts suivants :
  i. l'intégrité des données,
  ii. la confidentialité de l'information et des échanges,
  iii. la disponibilité des services,
  iv. l'authentification des utilisateurs et
  v. la non répudiation des transactions.

I. Normes de sécurité : les méthodes d'analyse des risques

A. Politique de sécurité

- Pour garantir la sécurité, une politique de sécurité est généralement organisée autour de 3 axes majeurs :

1. la sécurité physique des installations,
2. la sécurité logique du système d'information et
3. la sensibilisation des utilisateurs aux contraintes de sécurité.

I. Normes de sécurité : les méthodes d'analyse des risques

B. Audit

- Un audit de sécurité permet de mettre en évidence les faiblesses de la mise en œuvre d'une politique de sécurité.

- Le problème peut venir de la politique elle-même : mal conçue ou inadaptée aux besoins de l'entreprise, ou bien d'erreurs quand à sa mise en application.

- Des audits sont nécessaires : suite à la mise en place initiale d'une politique de sécurité, puis régulièrement pour s'assurer que les mesures de sécurité sont mises à niveau et que les usages restent conformes aux procédures.

I. Normes de sécurité : les méthodes d'analyse des risques

C. Tableau comparatif des normes

Le tableau suivant liste les principales normes utilisées provenant des organismes de normalisation internationaux ainsi que celles soutenues par le secteur privé ou associatif :

Méthode	Création	Popularité	Auteur	Soutenue par	Pays	Outils disponibles	Etat
EBIOS	1995	***	DCSSI	Gouvernement	France	logiciel gratuit	
Melisa		**	DGA	Armement	France		abandonnée
Marion	1980	**	CLUSIF	Association	France		abandonnée
Mehari	1995	***	CLUSIF	Association	France	logiciel Risicare	
Octave	1999	**	Université de Carnegie Mellon	Universitaire	Etats-Unis	logiciel payant	
Cramm	1986	**	Siemens	Gouvernement	Angleterre	logiciel payant	
SPRINT	1995	*	ISF	Association	Angleterre	logiciel payant	
BS 7799		***		Gouvernement	Angleterre		
ISO 17799		***		International			

I. Normes de sécurité : les méthodes d'analyse des risques

D. Présentation des principales normes

1. EBIOS

- EBIOS (**E**xpression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité) permet d'identifier les risques d'un SI et de proposer une politique de sécurité adaptée aux besoins de l'entreprise.

- Elle a été créée par la DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), du Ministrère de la Défence (France).

- La méthode EBIOS se compose de 5 guides (*Introduction*, *Démarche*, *Techniques*, *Outillages*) et d'un logiciel permettant de simplifier l'application de la méthodologie explicitée dans ces guides.

- Le logiciel libre et gratuit (les sources sont disponibles) permet de simplifier l'application de la méthode et d'automatiser la création des documents de synthèse.

I. Normes de sécurité : les méthodes d'analyse des risques

D. Présentation des principales normes

1. EBIOS

- **.....**
- La méthode EBIOS est découpée en 5 étapes :
    1. étude du contexte
    2. expression des besoins de sécurité
    3. étude des menaces
    4. identification des objectifs de sécurité
    5. détermination des exigences de sécurité

- EBIOS fournit donc la méthode permettant de construire une politique de sécurité en fonction d'une analyse des risques qui repose sur le contexte de l'entreprise et des vulnérabilités liées à son SI.

I. Normes de sécurité : les méthodes d'analyse des risques

D. Présentation des principales normes

2. Melisa

- Melisa (Méthode d'évaluation de la vulnérabilité résiduelle des systèmes d'information) fut inventée par Albert Harari au sein de la Direction Générale de l'Armement (DGA/DCN) en France.

- Melisa a été abandonnée par ses propriétaires bien qu'elle fut largement utilisée en France.

- Melisa est une méthode assez lourde basée sur un thésaurus de questions.

- Elle a vocation à être utilisée par de grandes entreprises.

- En raison de son abandon, cette méthode ne sera pas traitée en détail .

I. Normes de sécurité : les méthodes d'analyse des risques

D. Présentation des principales normes

3. Marion

- Marion (Méthodologie d'Analyse de Risques Informatiques Orientée par Niveaux) a été développée par le CLUSIF dans les années 1980 mais a été abandonnée en 1998 au profit de la méthode Mehari.

- C'est une méthode d'audit de la sécurité d'une entreprise, elle ne permet pas de mettre en oeuvre une politique de sécurité en tant que tel.

- A base d'un questionnaire, elle donne une évaluation chiffrée du risque informatique.
- Marion repose sur l'évaluation des aspects organisationnels et techniques de la sécurité de l'entreprise à auditer.
- Elle utilise 27 indicateurs classés en 6 thématiques. Chaque indicateur se voit attribuer une note entre 0 (insécurité) et 4 (excellent), la valeur 3 indiquant une sécurité correcte.

I. Normes de sécurité : les méthodes d'analyse des risques

D. Présentation des principales normes

3. Marion

- La méthode Marion définit 17 types de menaces :

Accidents physiques	***Erreur de saisie***
Malveillance physique	***Erreur de transmission***
Carence de personnel	***Erreur de conception / développement***
Carence de prestataire	***Erreur de transmission***
Panne du SI	***Erreur d'exploitation***
Interruption de fonctionnement du réseau	***Vice caché d'un progiciel***
Détournement de fonds	***Copie illicite de logiciels***
Détournement de biens	***Indiscrétion / détournement d'information***
Sabotage immatériel	***Attaque logique du réseau***

- Cette méthode est assez simple et peu complète.
- La méthode Mehari qui lui succède va plus loin en proposant la création complète de la politique de sécurité.

I. Normes de sécurité : les méthodes d'analyse des risques

D. Présentation des principales normes

3. Mehari

- Mehari (MEthode Harmonisée d'Analyse de RIsques) elle est dérivée des méthodes Melisa et Marion.

- Existant en langue française et en anglais, elle est utilisée par de nombreuses entreprises publiques ainsi que par le secteur privé.

- Le logiciel RISICARE développé par la société BUC SA est un outil de gestion des risques basé sur la méthode Mehari.

- La démarche générale de Mehari consiste en l'analyse des enjeux de sécurité. Ces enjeux expriment les dysfonctionnements ayant un impact direct sur l'activité de l'entreprise. Puis, des audits identifient les vulnérabilités du SI. Et enfin, l'analyse des risques proprement dite est réalisée.

I. Normes de sécurité : les méthodes d'analyse des risques

D. Présentation des principales normes

3. Mehari

- Mehari s'articule autour de 3 types de livrables :
  1. le Plan Stratégique de Sécurité (PSS)
  2. les Plans Opérationnels de Sécurité (POS)
  3. le Plan Opérationnel d'Entreprise (POE)

- Mehari apporte une démarche centrée sur les besoins de continuité d'activité de l'entreprise et fournit des livrables types aidés d'un guide méthodologie.
- Les audits qu'elle propose permettent la création de plan d'actions concrets.
- Cette méthode permet donc de construire une politique de sécurité destinée à pallier les vulnérabilités constatées lors des audits du *Plans Opérationnels de Sécurité* et d'atteindre le niveau de sécurité correspondant aux objectifs fixés dans le *Plan Stratégique de Sécurité*.

I. Normes de sécurité : les méthodes d'analyse des risques

E. Critères de choix

Comment choisir une méthode parmi le panel existant ? Sur quels critères faire ce choix ?

La liste suivante donne quelques pistes pour faciliter ce choix :

1. Critères de choix d'une méthode d'analyse des risques
2. l'origine géographique de la méthode, la culture du pays jouant beaucoup sur le fonctionnement interne des entreprises et leur rapport au risque
3. la langue de la méthode, il est essentiel de maîtriser le vocabulaire employé
4. l'existence d'outils logiciels en facilitant l'utilisation
5. l'existence d'un club d'utilisateurs afin d'avoir un retour d'expériences
6. la qualité de la documentation
7. la facilité d'utilisation et le pragmatisme de la méthode
8. la compatibilité avec une norme nationale ou internationale
9. le coût de la mise en œuvre
10. la quantité de moyens humains qu'elle implique et la durée de mobilisation
11. la taille de l'entreprise à laquelle elle est adaptée

II. LES OUTILS DE GESTION DE LA PROTECTION DES DP

A. Politique de gestion des risques

- La gestion des risques, même minimale, devrait être constituée des quatre étapes suivantes :

1. **Recenser les traitements** de données à caractère personnel, automatisés ou non, les données traitées (ex : fichiers client, contrats) et les supports sur lesquels elles reposent (les matériels, les logiciels, les canaux de communication, les supports papier).

2. **Apprécier les risques**

Risques	Impacts sur les personnes	Principales sources de risques	Principales menaces	Mesures existantes ou prévues	Gravité	Vraisem-blance
Accès illégitime à des données						
Modification non désirée de DP						
Disparition de données						

3. **Mettre en œuvre et vérifier les mesures prévues;** il convient de s'assurer qu'elles soient appliquées et contrôlées.

4. **Faire réaliser des audits de sécurité périodiques.** Chaque audit devrait donner lieu à un plan d'action dont la mise en œuvre devrait être suivie au plus haut niveau de l'organisme.

II. LES OUTILS DE GESTION DE LA PROTECTION DES DP

B. ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES : PIA

(Privacy Impact Assessment)

i. Le modèle d'analyse d'impact relatif a la protection des données personnelles de l'APDP du Bénin

- L'APDP élaboré puis publié un modèle d'analyse d'impact manuel téléchargeable sur son site (https://www.apdp.bj).

- Il s'agit d'un formulaire qui récapitule tous les aspects liés à la sécurité des DP avec des indicateurs d'appréciations

- Ce modèle proposé fournit donc la méthode permettant de construire une politique de sécurité en fonction d'une analyse des risques qui repose sur le contexte de l'entreprise et des vulnérabilités liées à son SI.

II. LES OUTILS DE GESTION DE LA PROTECTION DES DP

B. ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES : PIA
(Privacy Impact Assessment)

-

i. Le modèle d'analyse d'impact relatif a la protection des données personnelles de l'APDP du Bénin

- Le modèle d'analyse d'impact de l'APDP du Bénin est découpé en 4 étapes :

I. **Etude du contexte**
II. **Etude des principes fondamentaux**
III. **Etude des risques liés à la sécurité des données**
IV. **Validation de l'Analyse d'Impact**

II. LES OUTILS DE GESTION DE LA PROTECTION DES DP

B. ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES : PIA
(Privacy Impact Assessment)

i. Le modèle d'analyse d'impact relatif a la protection des données personnelles de l'APDP du Bénin

Cliquer Sur le Lien

LE FORMULAIRE D'ANALYSE D'IMPACT RELATIF A LA PROTECTION DES DONNÉES PERSONNELLES

II. LES OUTILS DE GESTION DE LA PROTECTION DES DP

B. ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES : PIA

(Privacy Impact Assessment)

ii. Exemple d'un outil logiciel l'analyse d'impact

- Le logiciel open source PIA développé par la CNIL française, facilite la conduite et la formalisation d'analyses d'impact relatives à la protection des données (AIPD) telles que prévues par le RGPD.

- L'Outil PIA est téléchargeable à partir du site de la CNIL.

- Le logiciel PIA s'inscrit dans une démarche d'accompagnement des responsables de traitement dans la mise en œuvre des obligations du RGPD.

- Disponible en 20 langues, il facilite et accompagne la conduite d'une analyse d'impact relative à la protection des données (AIPD), qui est obligatoire pour certains traitements.

II. LES OUTILS DE GESTION DE LA PROTECTION DES DP

B. ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES : PIA

(Privacy Impact Assessment)

- **À qui s'adresse l'outil PIA ?**

- L'outil s'adresse principalement aux responsables de traitement n'étant pas ou peu familiers avec la démarche d'analyse d'impact relative à la protection des données (AIPD).

- Il s'agit d'une version « prête à l'emploi », se lançant facilement sur un poste de travail.

- Il est aussi possible de déployer l'outil sur des serveurs afin de l'intégrer dans les outils déjà déployés en interne dans une entreprise.

II. LES OUTILS DE GESTION DE LA PROTECTION DES DP

B. ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES : PIA

(Privacy Impact Assessment)

- **Qu'est-ce que l'outil PIA ?**

L'outil PIA s'articule autour de trois axes afin de vous aider à suivre la méthode AIPD développée par la CNIL;

1. UNE BASE DE CONNAISSANCE JURIDIQUE ET TECHNIQUE

L'outil inclut les points juridiques qui garantissent la licéité du traitement, ainsi que les mesures protectrices des droits des personnes concernées.

Il dispose aussi d'une base de connaissance contextuelle accessible à tout moment lors de la réalisation de votre analyse et dont les contenus, reposant sur le RGPD ainsi que sur les guides AIPD et le guide sécurité de la CNIL, s'adaptent aux éléments étudiés du traitement.

II. LES OUTILS DE GESTION DE LA PROTECTION DES DP

B. ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES : PIA

(Privacy Impact Assessment)

- **Qu'est-ce que l'outil PIA ?**

2. UN OUTIL MODULAIRE POUR S'ADAPTER À VOS BESOINS

Afin de faciliter vos démarches de mise en conformité, vous pouvez adapter les contenus de l'outil à vos besoins spécifiques ou à votre secteur d'activité, par exemple en créant un modèle d'AIPD qu'il sera possible de dupliquer et utiliser pour des traitements de nature similaire.

Il vous est possible de modifier le code source de l'outil, publié sous licence libre, afin d'y ajouter des fonctionnalités ou bien l'intégrer à des outils déjà publiés en interne.

-

II. LES OUTILS DE GESTION DE LA PROTECTION DES DP

B. ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES : PIA

(Privacy Impact Assessment)

- **Qu'est-ce que l'outil PIA ?**

3. UNE INTERFACE DIDACTIQUE POUR RÉALISER VOS AIPD

- L'outil repose sur une interface ergonomique, vous permettant de gérer l'ensemble de vos analyses d'impact simplement.

- Il déroule clairement la méthode d'analyse d'impact de la CNIL, vous permettant ainsi de la suivre pas à pas et de n'en oublier aucune étape.

- Plusieurs outils de visualisation vous permettent de comprendre en un coup d'œil l'état des risques du traitement étudié.

II. LES OUTILS DE GESTION DE LA PROTECTION DES DP

B. ANALYSE D'IMPACT SUR LA PROTECTION DES DONNEES : PIA
(Privacy Impact Assessment)

- **Qu'est-ce que l'outil PIA ?**

- Version logicielle (3.0.2) **se télécharge et s'installe sur votre poste de travail.**

  - Disponible pour les systèmes d'exploitation suivants :
    - ✓ Windows (32 et 64 bits)
    - ✓ Linux (64 bits)
    - ✓ Mac OS

  - Version web

CONCLUSION

- Comme vous avez pu le constater , il existe de nombreuses méthodes d'analyse des risques, certaines simples d'utilisation, avec parfois des outils logiciels qui simplifient l'utilisation.

- D'autres méthodes sont réservées à des grands comptes du fait de leur complexité et des ressources humaines impliquées.

- Il vous reste à choisir la méthode qui s'applique le mieux à votre entreprise ou organisme public.

Merci pour votre aimable attention

Veuillez retrouver le présent slide : https://apdp.bj/formation-des-dpo-2021/

Pour plus de renseignements rendez-vous sur le site de l’APDP aux liens suivants :

- https://www.apdp.bj
- https://apdp.bj/les-outils-de-la-conformite/
- https://apdp.bj/procedures/