La Méthode EBIOS désormais adaptée aux traitements de données à caractère personnel et à la CNIL | Denis JACOPINI



La Méthode EBIOS, élaborée par l'ANSSI, initialement prévue pour la gestion des risques informatiques a été adaptée aux traitements de données personnelles Parmi les méthodes d'identification des risques en sécurité Informatique, la méthode EBIOS a été retenue par la CNIL en raison de sa simplicité de mise en oeuvre.

1. Objectifs

Dans une entreprise, les risques liée à l'utilisation de l'outils informatique peuvent être classés en deux principales catégories :

– Les risques liés au fonctionnement de l'outil informatique et à la sécurité d'accès au système;

- les risques liés à l'usage des données présentes dans le système informatique.

La gestion du premier risque est en général déléguée au responsable informatique ou, pour des structures de taille plus importantes, au Directeur ou Responsable des services

d’information (DSI) et, pour des structures de tailles encore plus importantes, confiée au Responsable de la Sécurité des Services d’Information.
Dans la longue liste des recommandations liées à la gestion de ces risques nous trouvons la gestion du fonctionnement du système informatique, la sécurité des données (garantie de pérennité et protection contre la fuite de de données) mais aussi la sécurité du système informatique contre les erreurs de manipulations et actes malveillants.

Par contre, la gestion des risques liés à l’usages des données, et plus particulièrement des données personnelles, est répartie entre l’utilisateur, le responsable des traitements (souvent le chef d’entreprise dans des structures de petite taille) et le correspondant Informatique et libertés.

Si l’utilisateur doit bien veiller à une utilisation responsable en évitant par exemple de quitter son poste sans verrouiller l’ordinateur

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l’hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d’informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

2. Introduction à la méthode EBIOS

Parmi les méthodes d'identification des risques en sécurité Informatique, la méthode EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité) a été retenue par la CNIL en raison de sa simplicité de mise en oeuvre.

La méthode, élaborée et tenue à jour par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information), en charge notamment, de la protection de l'état, initialement prévue pour être utilisée dans l'analyse de systèmes informatiques complexes, a été simplifiée et adaptée par la CNIL aux traitements de données personnelles et à la protection de la vie privée qui lui est associée

Cet article décrit les étapes de la démarche à appliquer pour réaliser une étude des risques qu'un traitement de Données à Caractère Personnel fait peser sur la vie privée. Il décrit la

manière d’employer la méthode EBIOS dans le contexte spécifique « informatique et libertés ».

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l’hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d’informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

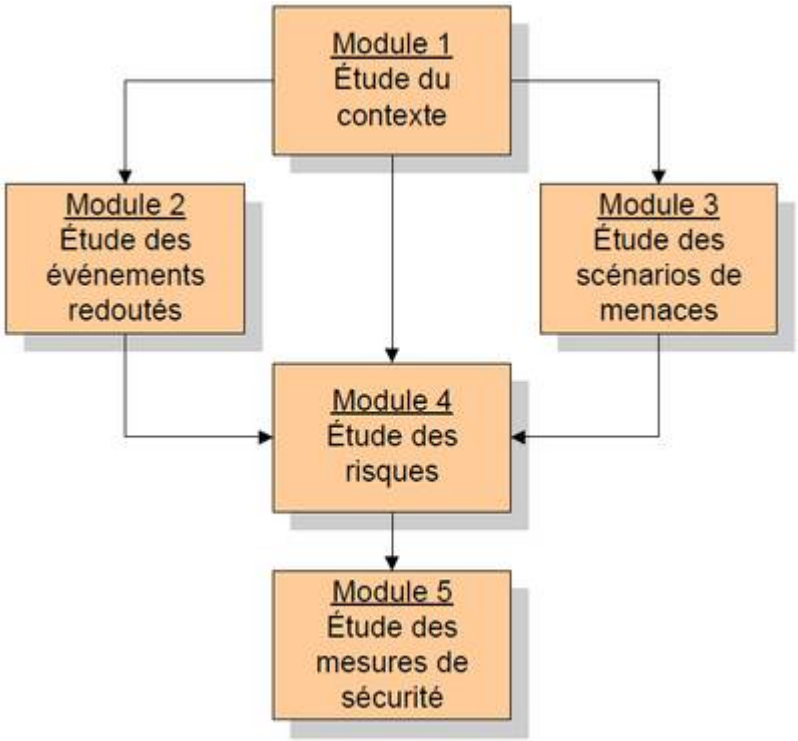
---

3. Les 5 étapes essentielles

On souhaite éviter les situations suivantes :

- indisponibilité des processus ;
- modification du traitement (détournement de la finalité, collecte excessive ou déloyale…) ;
- accès illégitime aux Données à Caractère Personnel ;
- modification non désirée des Données à Caractère Personnel ;
- disparition des Données à Caractère Personnel ;

La méthode EBIOS consiste, en fonction de l'environnement de départ, à décomposer en 5 étapes (que nous allons étudier en détail) permettant de passer en revue l'ensemble des mesures préconisées dans leur domaine spécifique, en repérer les points de faiblesses c'est-à-dire les vulnérabilités, d'estimer via une étude de risque, les capacités que semblent avoir les sources de risques à exploiter les vulnérabilités pour réaliser une menace, et enfin de mettre en place des mesures techniques et organisationnelles permettant de remédier aux vulnérabilités qu'elle peut présenter.



1. Etude du contexte :
   Quel est le sujet de l’étude ?
   Pourquoi et comment va-t-on gérer les risques ?

2. Étude des événements redoutés :
Quels sont les événements craints ?
Quels seraient les plus graves ?

3. Étude des menaces :
Quels sont les scénarios possibles ?
Quels sont les plus vraisemblables ?

4. Étude des risques :
Quelle est la cartographie des risques ?
Comment choisis-t-on de les traiter ?

5. Étude des mesures de sécurité :
Quelles mesures devrait-on appliquer ?
Les risques résiduels sont-ils acceptables ?

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l’hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d’informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

---

4. Les 5 étapes en détail

4.1. Etude du contexte : De quoi parle t-on ?

Le but de cette étape est d'obtenir une vision claire du périmètre considéré en identifiant tous les éléments utiles à la gestion des risques, en répondant aux questions suivantes :

4.1.1 Quels sont les éléments à protéger ?

- Quel est le traitement concerné ?
- Quelle est sa finalité (voir les articles 6 et 9 de la loi Informatique et Libertés)?
- Quels sont ses destinataires ?
- Quel est le processus métier que le traitement permet de réaliser ?

- Quelles sont les personnes concernées par le traitement ?
- Comment les processus légaux vont-ils être mis en oeuvre ?
- Quelles sont les DCP du traitement considéré ?
- Quelles sont les DCP utilisées par les processus légaux ?

4.1.2 Quels sont les supports des éléments à protéger ?

- Quels sont les matériels (ordinateurs, routeurs, supports électroniques…) ?
- Quels sont les logiciels (systèmes d'exploitation, messagerie, base de données, applications métier…) ?
- Quels sont les canaux informatiques (câbles, WiFi, fibre optique…) ?
- Quelles sont les personnes impliquées?
- Quels sont les supports papier (impressions, photocopies…) ?
- Quels sont les canaux de transmission papier (envoi postal, circuit de validation…) ?

4.1.3 Quels sont les principaux bénéfices du traitement pour les personnes concernées ou la société en général ?

4.1.4 Quelles sont les principales références à respecter (réglementaires, sectorielles…) ?

4.1.5 Quelles sont les sources de risques pertinentes qui peuvent être à l'origine de risques dans le contexte particulier du traitement considéré ?

- Quelles sont les personnes internes à considérer (utilisateur, administrateur,
- développeur, décideur…) ?
- Quelles sont les personnes externes à considérer (client, destinataire, prestataire,
- concurrent, militant, curieux, individu malveillant, organisation gouvernementale,
- activité humaine environnante…) ?
- Quelles sont les sources non humaines à considérer (sinistre, code malveillant
- d'origine inconnue, phénomène naturel, catastrophe naturelle ou sanitaire…) ?

4.2 Étude des événements redoutés : Que craint-on qu'il arrive ?

Le but de cette étape est d'obtenir une liste explicite et hiérarchisée de tous les événements redoutés dans le cadre du traitement considéré et d'en mesurer leur valeur de danger.
Pour expliciter les événements redoutés, leurs impacts potentiels doivent être identifiés :
quelles pourraient être les conséquences sur l'identité des personnes concernées, leur vie privée, les droits de l'homme ou les libertés publiques pour chacun des événements redoutés, c'est-à-dire si :

- les processus légaux n'étaient pas disponibles ?
- le traitement était modifié ?
- une personne non autorisée accédait aux DCP ?
- les DCP étaient modifiées ?
- les DCP disparaissaient ?

Afin de hiérarchiser les événements redoutés, la gravité est déterminée en mesurer la facilité avec laquelle on peut identifier les personnes concernées et l'importance des dommages des impacts potentiels.

Avec quelle facilité peut-on identifier les personnes concernées ? (1 à 4)

- 1. Négligeable : il semble quasiment impossible d'identifier les personnes à l'aide des Données à Caractère Personnel les concernant (ex. : prénom seul à l'échelle de la population française).
- 2. Limité : il semble difficile d'identifier les personnes à l'aide des DCP les concernant, bien que cela soit possible dans certains cas (ex. : nom et prénom à l'échelle de la population française).
- 3. Important : il semble relativement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom et date de naissance, à l'échelle de la population française).
- 4. Maximal : il semble extrêmement facile d'identifier les personnes à l'aide des DCP les concernant (ex. : nom, prénom, date de naissance et adresse postale, à l'échelle de la population française).

Quelle serait l'importance des dommages correspondant à l'ensemble des impacts potentiels ? (1 à 4)

- 1. Négligeable : les personnes concernées ne seront pas impactées ou pourraient connaître quelques désagréments, qu'elles surmonteront sans difficulté (perte de temps pour réitérer des démarches ou pour attendre de les réaliser, agacement, énervement…).
- 2. Limité : les personnes concernées pourraient connaître des désagréments significatifs, qu'elles pourront surmonter malgré quelques difficultés (frais supplémentaires, refus d'accès à des prestations commerciales, peur, incompréhension, stress, affection physique mineure…).

- 3. Important : les personnes concernées pourraient connaître des conséquences significatives, qu'elles devraient pouvoir surmonter, mais avec de sérieuses difficultés (détournements d'argent, interdiction bancaire, dégradation de biens, perte d'emploi, assignation en justice, aggravation de l'état de santé…).
- 4. Maximal : les personnes concernées pourraient connaître des conséquences significatives, voire irrémédiables, qu'elles pourraient ne pas surmonter (péril financier tel que des dettes importantes ou une impossibilité de travailler, affection psychologique ou physique de longue durée, décès…).

Mesure de la gravité = Facilité d'identification des personnes + importance des dommages

Caractère identifiant + caractère préjudiciable	Gravité correspondante
< 5	1. Négligeable
= 5	2. Limité
= 6	3. Important
> 6	4. Maximal

4.3 Étude des menaces : Comment cela peut-il arriver ?

Cette étape est optionnelle si la gravité précédemment calculée est négligeable (1) ou limitée (2).

Le but de cette étape est d'obtenir une liste explicite et hiérarchisée de toutes les menaces qui permettraient aux événements redoutés de survenir.

Vulnérabilités des supports

Risque à anticiper :

- Détérioration d’un matériel (ex. : destruction d’un serveur)
- Usage anormal d’un logiciel (ex. : maladresse en manipulant les fichiers)
- Départ d’une personne (ex. : démission de celui qui connait les procédures)
- Disparition d’un canal papier (ex. : changement de procédures)
- Vol d’un matériel (ex. : vol d’un PC portable dans le train)
- Détournement d’usage d’un logiciel (ex. : usage à titre personnel)
- Modification d’un logiciel (ex. : propagation d’un virus)

Dans quelle mesure les caractéristiques des supports sont-elles exploitables pour réaliser la menace ?

- 1. Négligeable : il ne semble pas possible de réaliser la menace en s’appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l’organisme dont l’accès est contrôlé par badge et code d’accès).
- 2. Limité : il semble difficile de réaliser la menace en s’appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans un local de l’organisme dont l’accès est contrôlé par badge).
- 3. Important : il semble possible de réaliser la menace en s’appuyant sur les caractéristiques des supports (ex. : vol de supports papiers stockés dans les bureaux d’un organisme dont l’accès est contrôlé par une personne à l’accueil).

- 4. Maximal : il semble extrêmement facile de réaliser la menace en s'appuyant sur les caractéristiques des supports (ex. : vol de supports papier stockés dans le hall public de l'organisme).

Capacités des sources de risques sont estimées pour chaque menace

Quelles sont leurs capacités à exploiter les vulnérabilités (compétences, temps disponible, ressources financières, proximité du système, motivation, sentiment d'impunité…) ?

- 1. Négligeable : les sources de risques ne semblent pas avoir de capacités particulières pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne sans mauvaises intentions ayant des privilèges restreints).
- 2. Limité : les sources de risques ont quelques capacités, mais jugées peu importantes, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne mal intentionnée ayant des privilèges restreints).
- 3. Important : les sources de risques ont des capacités réelles, jugées importantes, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne sans mauvaises intentions ayant des privilèges d'administration illimités).
- 4. Maximal : les sources de risques ont des capacités certaines, jugées illimitées, pour réaliser la menace (ex. : détournement d'usage de logiciels par une personne mal intentionnée ayant des privilèges d'administration illimités).

Vraisemblance des menaces = Mesure de la vulnérabilités des supports + Capacités des sources de risques

Vulnérabilités des supports + capacités des sources de risques	Vraisemblance correspondante
< 5	1. Négligeable
= 5	2. Limité
= 6	3. Important
> 6	4. Maximal

Exemples de menaces qui peuvent affecter la confidentialité

Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
C01. Usage anormal d'un matériel	Utilisation de clefs USB ou disques inappropriés à la sensibilité des informations, utilisation ou transport d'un matériel sensible à des fins personnelles...	Utilisable en dehors de l'usage prévu...
C02. Espionnage d'un matériel	Observation d'un écran à l'insu de son utilisateur dans un train, photographie d'un écran, géolocalisation d'un matériel, captation de signaux électromagnétiques à distance...	Permet d'observer des données interprétables, émet des signaux compromettants...
C03. Modification d'un matériel	Piégeage par un keylogger, retrait d'un composant matériel, branchement d'un appareil (ex. : clé USB) pour lancer un système d'exploitation ou récupérer des données...	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions...) via des connecteurs (ports, slots...), permet de désactiver des éléments (port USB...)...
C04. Perte d'un matériel	Vol d'un ordinateur portable dans une chambre d'hôtel, vol d'un téléphone portable professionnel par un pickpocket, récupération d'un matériel ou d'un support mis au rebut, perte d'un support de stockage électronique...	Petite taille, attractif (valeur marchande)...
C05. Détournement d'usage d'un logiciel	Fouille de contenu, croisement illégitime de données, élévation de privilèges, effacement de traces, envoi de *spams* depuis la messagerie, détournement de fonctions réseaux...	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer...), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées...
C06. Analyse d'un logiciel	Balayage d'adresses et ports réseau, collecte de données de configuration, étude d'un code source pour déterminer les défauts exploitables, test des réponses d'une base de données à des requêtes malveillantes...	Possibilité d'observer le fonctionnement du logiciel, accessibilité et intelligibilité du code source...
C07. Modification d'un logiciel	Piégeage par un keylogger logiciel, contagion par un code malveillant, installation d'un outil de prise de contrôle à distance, substitution d'un composant par un autre...	Modifiable (améliorable, paramétrable...), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes...), ne fonctionne pas correctement ou conformément aux attentes...
C08. Écoute passive d'un canal informatique	Interception de flux sur le réseau Ethernet, acquisition de données sur un réseau wifi...	Perméable (émission de rayonnements parasites ou non), permet d'observer des données interprétables...
C09. Espionnage d'une personne à distance	Divulgation involontaire en conversant, écoute d'une salle de réunion avec un matériel d'amplification sensorielle...	Peu discret (loquace, sans réserve...), routinier (habitudes facilitant l'espionnage récurrent)...
C10. Manipulation d'une personne	Influence (hameçonnage, filoutage, ingénierie sociale, corruption...), pression (chantage, harcèlement moral...)...	Influençable (naïf, crédule, obtus, faible estime de soi, faible loyauté...), manipulable (vulnérable aux pressions sur soi ou son entourage)...
C11. Récupération d'une personne	Débauchage d'un employé, changement d'affectation, rachat de tout ou partie de l'organisation...	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel...
C12. Visualisation d'un document papier	Lecture, photocopie, photographie...	Permet d'observer des données interprétables...
C13. Vol d'un document papier	Vol de dossiers dans les bureaux, vol de courriers dans la boîte aux lettres, récupération de documents mis au rebut...	Portable...
C14. Espionnage d'un canal papier	Lecture de parapheurs en circulation, reproduction de documents en transit...	Observable...

Exemples de menaces qui peuvent affecter l'intégrité

Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
I01. Modification d'un matériel	Ajout d'un matériel incompatible menant à un dysfonctionnement, retrait d'un matériel indispensable au fonctionnement correct d'une application...	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions...) via des connecteurs (ports, slots...), permet de désactiver des éléments (port USB...)...
I02. Usage anormal d'un logiciel	Modifications inopportunes dans une base de données, effacement de fichiers utiles au bon fonctionnement, erreur de manipulation menant à la modification de données...	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer...), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées...
I03. Modification d'un logiciel	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre...	Modifiable (améliorable, paramétrable...), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes...), ne fonctionne pas correctement ou conformément aux attentes...
I04. Attaque du milieu via un canal informatique	*Man in the middle* pour modifier ou ajouter des données à un flux réseau, rejeu (réémission d'un flux intercepté)...	Permet d'altérer les flux communiqués (interception puis réémission, éventuellement après altération...), seule ressource de transmission pour le flux, permet de modifier les règles de partage du canal informatique (protocole de transmission qui autorise l'ajout de nœuds...)...
I05. Surcharge des capacités d'une personne	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences...	Ressources insuffisantes pour les tâches assignées, capacités inappropriées aux conditions de travail, compétences inappropriées à la fonction Incapacité à s'adapter au changement...
I06. Manipulation d'une personne	Influence (rumeur, désinformation...)...	Influençable (naïf, crédule, obtus...)...
I07. Falsification d'un document papier	Modification de chiffres dans un dossier, remplacement d'un document par un faux...	Falsifiable (support papier au contenu modifiable)...
I08. Manipulation d'un canal papier	Modification d'une note à l'insu du rédacteur, changement d'un parapheur par un autre, envoi multiple de courriers contradictoires...	Permet d'altérer les documents communiqués, seule ressource de transmission pour le canal, permet la modification du circuit papier ...

Exemples de menaces qui peuvent affecter la disponibilité

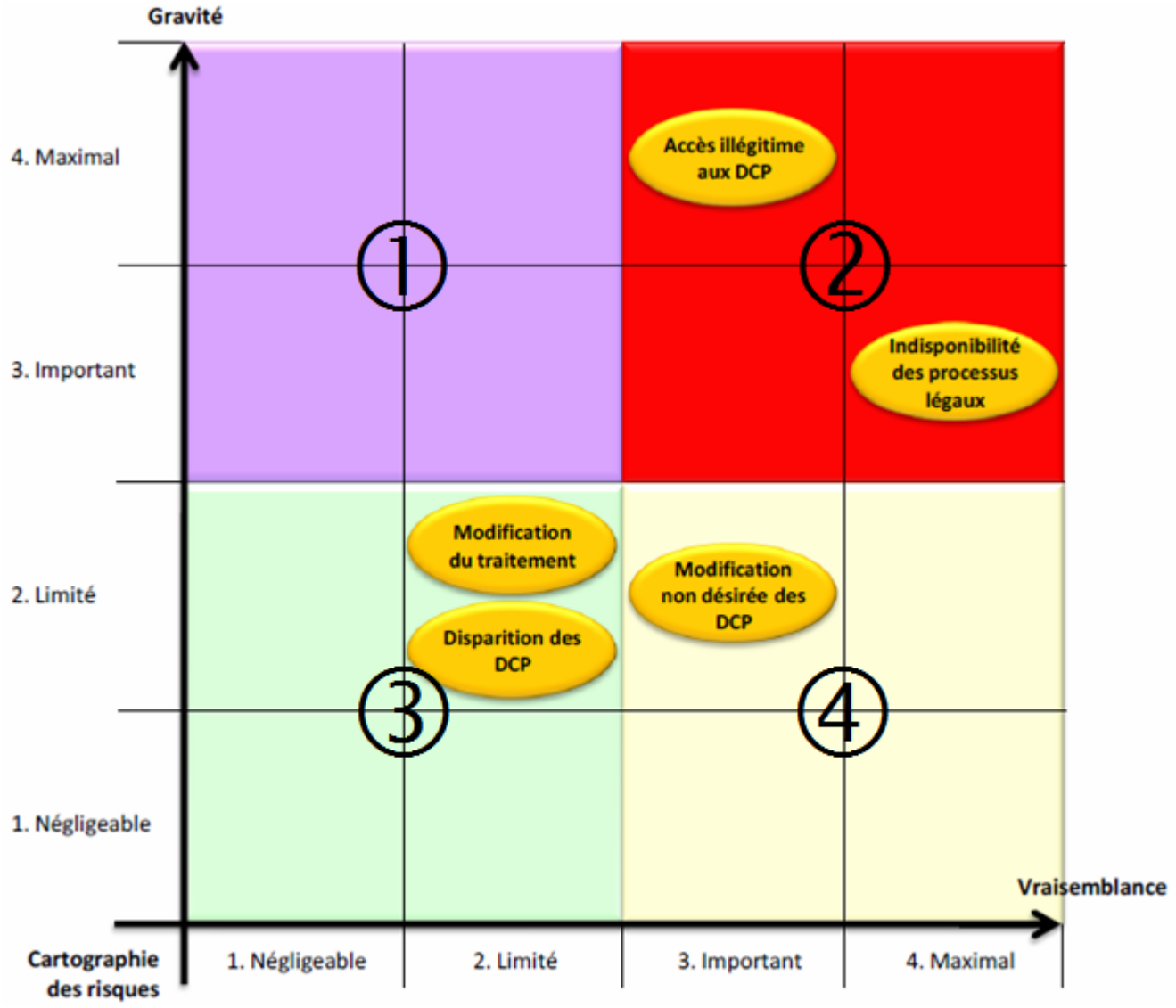
Menaces génériques	Exemples de menaces	Exemples de vulnérabilités des supports
D01. Détournement d'usage d'un matériel	Stockage de fichiers personnels, utilisation à des fins personnelles...	Utilisable en dehors de l'usage prévu...
D02. Dépassement des limites de fonctionnement d'un matériel	Unité de stockage pleine, panne de courant, surexploitation des capacités de traitement, échauffement, température excessive...	Dimensionnement inapproprié des capacités de stockage, dimensionnement inapproprié des capacités de traitement, n'est pas approprié aux conditions d'utilisation, requiert en permanence de l'électricité pour fonctionner, sensible aux variations de tension...
D03. Modification d'un matériel	Ajout d'un matériel incompatible menant à une panne, retrait d'un matériel indispensable au fonctionnement du système...	Permet d'ajouter, retirer ou substituer des éléments (cartes, extensions...) via des connecteurs (ports, slots...), permet de désactiver des éléments (port USB...)...
D04. Détérioration d'un matériel	Inondation, incendie, vandalisme, dégradation du fait de l'usure naturelle, dysfonctionnement d'un dispositif de stockage...	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement...) n'est pas approprié aux conditions d'utilisation ; effaçable (vulnérable aux effets magnétiques ou vibratoires...)...
D05. Perte d'un matériel	Vol d'un ordinateur portable, perte d'un téléphone portable, mise au rebut d'un support ou d'un matériel...	Portable, attractif (valeur marchande)...
D06. Usage anormal d'un logiciel	Effacement de données, utilisation de logiciels contrefaits ou copiés, erreur de manipulation menant à la suppression de données...	Donne accès à des données, permet de les manipuler (supprimer, modifier, déplacer...), peut être détourné de son usage nominal, permet d'utiliser des fonctionnalités avancées...
D07. Dépassement des limites d'un logiciel	Dépassement du dimensionnement d'une base de données, injection de données en dehors des valeurs prévues...	Permet de saisir n'importe quelle donnée, permet de saisir n'importe quel volume de données, permet d'exécuter des actions avec les données entrantes, peu interopérable...
D08. Modification d'un logiciel	Manipulation inopportune lors de la mise à jour, configuration ou maintenance, contagion par un code malveillant, substitution d'un composant par un autre...	Modifiable (améliorable, paramétrable...), maîtrise insuffisante par les développeurs ou les mainteneurs (spécifications incomplètes, peu de compétences internes...), ne fonctionne pas correctement ou conformément aux attentes...
D09. Suppression de tout ou partie d'un logiciel	Effacement d'un exécutable en production ou de code sources, bombe logique...	Possibilité d'effacer ou de supprimer des programmes, exemplaire unique, utilisation complexe (mauvaise ergonomie, peu d'explications...)...
D10. Perte d'un logiciel	Non renouvellement de la licence d'un logiciel utilisé pour accéder aux données...	Exemplaire unique (des contrats de licence ou du logiciel, développé en interne...), attractif (rare, novateur, grande valeur commerciale...), cessible (clause de cessibilité totale dans la licence...)...
D11. Saturation d'un canal informatique	Détournement de la bande passante, téléchargement non autorisé, coupure d'accès Internet...	Dimensionnement fixe des capacités de transmission (dimensionnement insuffisant de la bande passante, plage de numéros téléphoniques limitée...)...
D12. Dégradation d'un canal informatique	Sectionnement de câblage, mauvaise réception du réseau wifi...	Altérable (fragile, cassable, câble de faible structure, à nu, gainage disproportionné...), unique...
D13. Disparition d'un canal informatique	Vol de câbles de transmission en cuivre...	Attractif (valeur marchande des câbles...), transportable (léger, dissimulable...), peu visible (oubliable, insignifiant, peu remarquable...)...
D14. Surcharge des capacités d'une personne	Charge de travail importante, stress ou perturbation des conditions de travail, emploi d'un personnel à une tâche non maîtrisée ou mauvaise utilisation des compétences...	Ressources insuffisantes pour les tâches assignées capacités inappropriées aux conditions de travail, compétences inappropriées aux conditions d'exercice de ses fonctions, incapacité à s'adapter au changement...
D15. Atteinte d'une personne	Accident du travail, maladie professionnelle, autre blessure ou maladie, décès, affection neurologique, psychologique ou psychiatrique...	Limites physiques, psychologiques ou mentales...
D16. Départ d'une personne	Changement d'affectation, fin de contrat ou licenciement, rachat de tout ou partie de l'organisation...	Faible loyauté vis-à-vis de l'organisme, faible satisfaction des besoins personnels, facilité de rupture du lien contractuel...
D17. Effacement d'un document papier	Effacement progressif avec le temps, effacement volontaire de parties d'un texte...	Modifiable (support papier au contenu effaçable).
D18. Dégradation d'un document papier	Vieillissement de documents archivés, embrasement des dossiers lors d'un incendie...	Composants de mauvaise facture (fragile, facilement inflammable, sujet au vieillissement...), n'est pas approprié aux conditions d'utilisation...
D19. Disparition d'un document papier	Vol de documents, perte de dossiers lors d'un déménagement, mise au rebut...	Portable...
D20. Saturation d'un canal papier	Surcharge de courriers, surcharge d'un processus de validation...	Existence de limites quantitatives ou qualitatives..
D21. Dégradation d'un canal papier	Coupure du flux suite à une réorganisation, blocage du courrier du fait d'une grève...	Instable, unique...
D22. Modification d'un canal papier	Modification dans l'expédition des courriers Réorganisation de circuits papier, changement de langue professionnelle...	Modifiable (remplaçable...)...
D23. Disparition d'un canal papier	Réorganisation supprimant un processus, disparition d'un transporteur de documents...	Utilité non reconnue...

4.4 Étude des risques : quel est le niveau des risques ?

Le but de cette étape est d'obtenir une cartographie des risques permettant de décider de la priorité de traitement. Puisqu'un risque est composé d'un événement redouté et de toutes les menaces qui permettraient qu'il survienne :

- sa gravité est égale à celle de l'événement redouté,
- sa vraisemblance est égale à la valeur la plus élevée de la vraisemblance des menaces associées à l'événement redouté.

On peut dès lors positionner les risques sur une cartographie :



En fonction du positionnement de vos risques au sein de la cartographie ci-dessus, vous pouvez par ordre de priorité, vous fixer des objectifs :

Zone n°1 : La gravité des risques est élevée, mais la vraisemblance faible
Ces risques doivent être évités ou réduits, par l'application de mesures de sécurité diminuant leur gravité ou leur vraisemblance. Les mesures de prévention devront être privilégiées ;

Zone n°2 : La gravité et la vraisemblance sont élevées
Ces risques doivent absolument être évités ou réduits par l'application de mesures de sécurité diminuant leur gravité et leur vraisemblance. Dans l'idéal, il conviendrait même de s'assurer qu'ils sont traités à la fois par des mesures indépendantes de prévention (actions avant le sinistre), de protection (actions pendant le sinistre) et de récupération (actions après le sinistre) ;

Zone n°3 : La gravité et la vraisemblance sont faibles
Ces risques peuvent être pris, d'autant plus que le traitement des autres risques devrait également contribuer à leur traitement.

Zone n°4 : La gravité est faible mais la vraisemblance élevée
Ces risques doivent être réduits par l'application de mesures de sécurité diminuant leur vraisemblance. Les mesures de récupération devront être privilégiées ;

4.5 Étude des mesures de sécurité : Quelles mesures devrait-on appliquer ?

Le but de cette étape est de bâtir un dispositif de protection qui permette de traiter les risques de manière proportionnée, qui soit conforme à la Loi informatique et Libertés, et qui tienne compte des contraintes du responsable de traitement

(légales, financières, techniques…).

Tout d’abord, il convient de déterminer les mesures pour traiter les risques. Pour ce faire, il est nécessaire de relier les mesures existantes ou prévues (identifiées précédemment dans l’étude ou dans les références applicables) au(x) risque(s) qu’elles contribuent à traiter.

Des mesures sont ensuite ajoutées tant que le niveau des risques n’est pas jugé acceptable.

Cette action consiste à déterminer des mesures complémentaires qui vont porter :

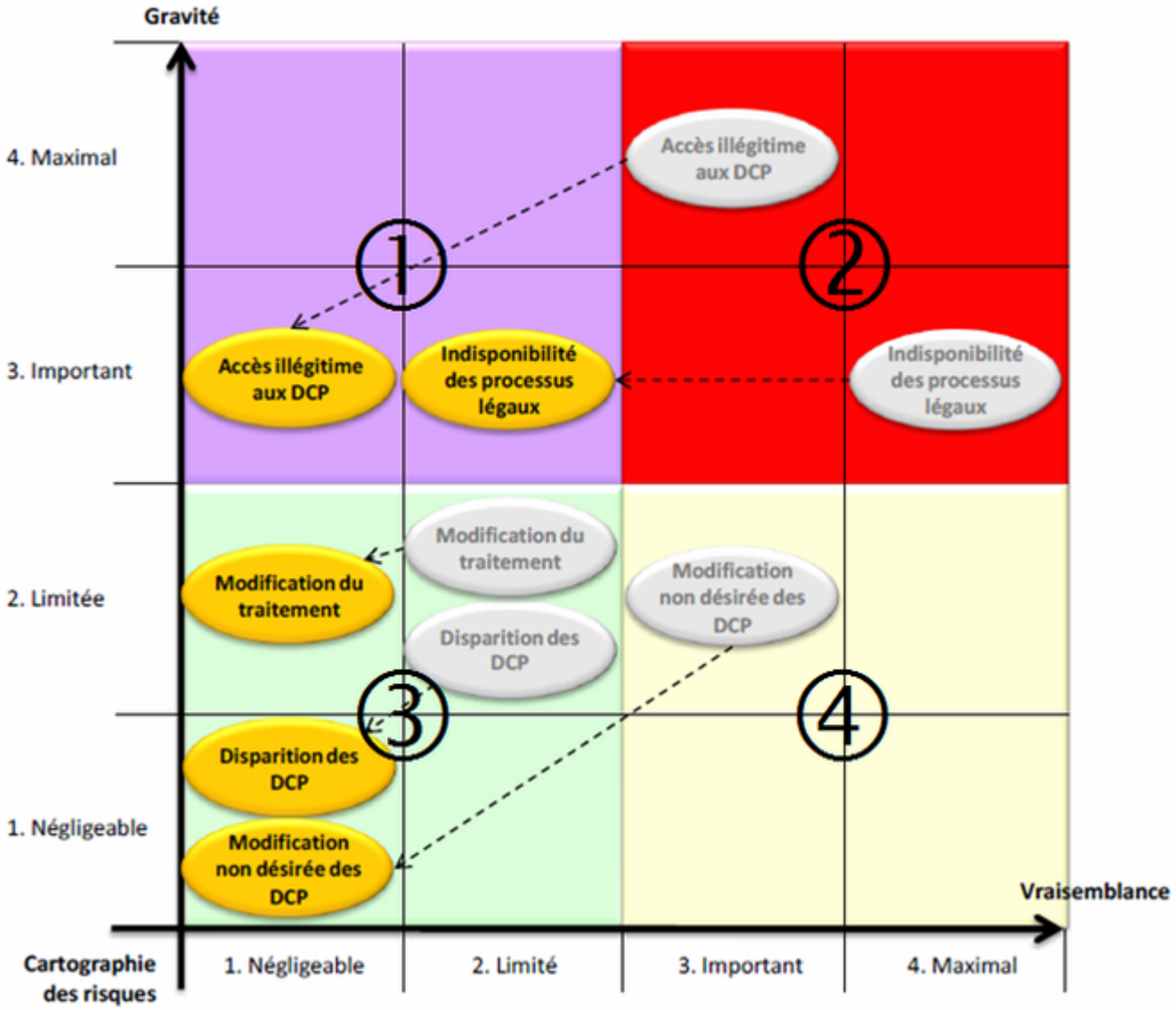
1. sur les éléments à protéger : mesures destinées à empêcher que leur sécurité ne puisse être atteinte, à détecter leur atteinte ou à recouvrer la sécurité informer les personnes concernées, minimiser les DCP, anonymiser les DCP…) ;
2. puis, si ce n’est pas suffisant, sur les impacts potentiels : mesures destinées à empêcher que les conséquences du risque ne puissent se déclarer, à identifier et limiter leurs effets ou à les résorber (sauvegarder, contrôler l’intégrité, gérer les violations de DCP…) ;
3. ensuite, si ce n’est pas suffisant, sur les sources de risques : mesures destinées à les empêcher d’agir ou de concrétiser le risque, à identifier et limiter leur action ou à se retourner contre elles (contrôler les accès physiques et logiques, tracer l’activité, gérer les tiers, lutter contre les codes malveillants…) ;
4. enfin, si ce n’est pas suffisant, sur les supports : mesures destinées à empêcher que les vulnérabilités puissent être exploitées, à détecter et limiter les menaces qui surviennent tout de même ou à retourner à

l’état de fonctionnement normal (réduire les vulnérabilités des logiciels, des matériels, des personnes, des documents papiers…).

Remarque :

Plus les capacités des sources de risques sont importantes, plus les mesures doivent être robustes pour y résister.
Par ailleurs, les éventuels incidents qui auraient déjà eu lieu, notamment les violations de DCP, ainsi que les difficultés rencontrées pour mettre en oeuvre certaines mesures, peuvent servir à améliorer le dispositif de sécurité.
Les mesures spécifiées devraient être formalisées, mises en place, auditées de manière régulière et améliorées de manière continue.

Il convient ensuite de ré-estimer la gravité et la vraisemblance des risques résiduels (c’est-à dire les risques qui subsistent après application des mesures choisies) en tenant compte de ces mesures complémentaires. Il est alors possible de les repositionner sur la cartographie ci-dessous :



Enfin, il convient d'expliquer pourquoi les risques résiduels peuvent être acceptés.

Cette justification peut s'appuyer sur les nouveaux niveaux de gravité et de vraisemblance et sur les bénéfices du traitement identifiés précédemment (prise de risques au regard des bénéfices attendus) en appliquant les règles suivantes :

Zone n°1 : Risques dont la gravité est élevée mais la vraisemblance faible
Ces risques peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur gravité et

si leur vraisemblance est négligeable ;

Zone n°2 : Risques dont la gravité et la vraisemblance sont élevées
Ces risques ne doivent pas être pris ;

Zone n°3 : Risques dont la gravité et la vraisemblance sont faibles
Ces risques peuvent être pris.

Zone n°4 : Risques dont la gravité est faible mais la vraisemblance élevée : ces risques peuvent être pris, mais uniquement s'il est démontré qu'il n'est pas possible de réduire leur vraisemblance et si leur gravité est négligeable ;

Remarque :

Il peut être acceptable de déroger à ces règles, mais uniquement s'il est démontré que les
bénéfices du traitement sont largement supérieurs aux risques.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Références :

http://www.cnil.fr/fileadmin/documents/Guides_pratiques/CNIL-Guide_Securite_avance_Methode.pdf
http://www.ssi.gouv.fr/fr/guides-et-bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html

---

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Cet article vous à plu ? Laissez-nous un commentaire (notre source d’encouragements et de progrès)