# GUIDE DE BONNES PRATIQUES


# LES PETITES ET MOYENNES ENTREPRISES MAROCAINES, COMMENT FAIRE FACE AUX MENACES CYBERNETIQUES ?

Edition 2018


Les Petites et Moyennes Entreprises Marocaines, Comment faire face aux menaces cybernétiques? – 2018



Dépôt légal - Bibliothèque Nationale du Royaume du Maroc, 2017

# Les Petites et Moyennes Entreprises Marocaines, Comment faire face aux menaces cybernétiques ?

Guide de bonnes pratiques

# Présentation de l'AUSIM

L'Association des Utilisateurs des Systèmes d'Informations au Maroc (AUSIM) est une association à but non lucratif créée en avril 1993.

Comptant parmi ses adhérents nombre de structures de premier plan au niveau organisationnel et managérial (Offices, Banques, Assurances, Entreprises Industrielles,…), l'AUSIM œuvre activement dans l'esprit de développer et de vulgariser l'usage des Technologies de l'Information au Maroc.

A ce titre, elle a pour objectifs :

- L'échange d'expériences et d'informations d'ordre technique, scientifique et culturel entre les adhérents et ce par l'organisation de rencontres, de séminaires et de conférences, aussi bien au Maroc qu'à l'étranger.
- L'étude et la sauvegarde, en cas de besoin, des intérêts généraux, à caractère technique, économique et financier, de ses adhérents.
- La création et l'entretien des rapports de bonne fraternité entre ses membres et le renforcement des liens avec d'autres associations similaires, au Maroc et à l'étranger.
- L'entraide mutuelle au niveau des exploitations des systèmes des logiciels.
- La diffusion des connaissances et des informations relatives au secteur des Systèmes d'Information.
- La participation active aux principales réformes nationales et sectorielles ayant trait aux Technologies de l'Information.

# Présentation du CMRPI

Le Centre Marocain de Recherches Polytechniques et d'Innovation (CMRPI) est une Association Savante Marocaine, positionnée dans l'optique recherche, développement et innovation et est à but non lucratif, fondée en Juin 2012 et qui a la mission de :

- Rassembler des personnes physiques et morales concernées par les sciences et techniques dans plusieurs domaines de l'industrie et de la recherche scientifique
- Faciliter l'implication des chercheurs marocains, de l'intérieur du pays et également à l'étranger, dans la contribution au développement du Maroc
- Contribuer dans le transfert du savoir vers le milieu socio-économique national et international
- Distinguer parmi ses membres les meilleurs spécialistes dans chaque domaine
- Favoriser des contacts fréquents avec d'autres membres, dans leurs spécialités ou hors de leurs spécialités, tout particulièrement pour les plus jeunes
- Développer une importante source d'informations spécialisées
- Constituer une tribune qui permette à ses membres de faire connaître leur point de vue et leurs travaux
- Représenter l'ensemble de ses membres auprès d'autres sociétés scientifiques et techniques marocaines ou étrangères.

L' activité du Centre Marocain de Recherches Polytechniques et d'Innovation, est en grande partie liée à celle de la recherche appliquée dans le domaine des hautes technologies. Le CMRPI est aussi en relation étroite avec les services et organismes d'Etat. Cependant, le CMRPI offre à la société savante et universitaire, pour la genèse et la diffusion des idées, une voie distincte de l'industrie et des instances gouvernementales. Ce qui rendra utilisables ou commercialisables les résultats, les connaissances et les compétences de la recherche.
Par les moyens d'expression offerts à ses membres, qu'ils soient universitaires, experts, chercheurs, ingénieurs ou étudiants, le CMRPI leur permet de faire connaître leurs travaux, leurs points de vue, leurs productions ou leurs aspirations.

# Préface

A l'ère de la Disruption Digitale ou les technologies numériques accélèrent l'expansion du volume des données informatiques et l'utilisation massive de logiciels dans la vie quotidienne, et Face à la prolifération des menaces informatiques, il est devenu crucial pour chaque entreprise de se protéger au mieux des cyberattaques et d'adopter une stratégie de sécurité globale pour sauvegarder son patrimoine informationnel et assurer la pérennité de son business.

On ne compte plus les études alarmantes sur le nombre d'attaques informatiques par seconde contre des sociétés ou les millions de dollars perdus lors d'offensives de hackers, et Il n'y a pas de profil type d'entreprise particulièrement visée par des attaques. Toute entreprise qui traite des données doit mettre la sécurité au centre de ses préoccupations et instaurer un système de management de la sécurité en fonction de sa taille et de la criticité de son business.

C'est dans cette optique, que ce guide de bonnes pratiques insiste sur les questions d'organisation et de capital humain, au-delà de la technologie.

AUSIM beyond digital

**Rachid BAARBI,**
**CIO Assurances Lyazidi**
**Administrateur AUSIM**

Faire face à la cybercriminalité, c'est au-delà de la technologie, c'est avant tout un comportement humain et ensuite une maîtrise de la sécurité des infrastructures technologiques et des données qui devient aujourd'hui de plus en plus compliquée, vue l'évolution de nouveaux vecteurs intelligents de cyber-attaque, c'est pour cette raison que la cybersécurité des PME, entant que discipline et science, vient pour assister les mangers, les responsables du management et sécurité des systèmes d'information, et également les utilisateurs, pour la mise en place d'une stratégie efficace et globale de la protection des données et des infrastructures de l'entreprise, afin d'assurer sa transformation digitale.

Ce guide de sensibilisation, fruit de collaboration de plusieurs experts et intervenants de l'écosystème de la cybersécurité au Maroc, propose les grandes lignes de base nécessaires, mais certainement non suffisantes, pour la mise en place d'une stratégie de cybersécurité dans une petite ou moyenne entreprise, il rappelle alors les normes internationales de sécurité IT et aussi le cadre législatif et juridique marocain et international. Merci pour tous ceux qui ont participé de proche ou de loin pour la réalisation et l'amélioration de ce guide, bien notamment l'AUSIM.

CMRPI

**Pr. Youssef Bentaleb,**
**Président du CMRPI**
**Directeur de la Campagne Nationale**
**de Lutte Contre la Cybercriminalité**
**CNLCC 2014-2017**

# Sommaire

# Sommaire

# Préambule

La Cybersécurité devient un facteur de compétitivité et donc de croissance pour les entreprises. Elle est par ailleurs, un moyen d'être à l'abri d'une respon-sabilité civile ou pénale qui peut être engendrée suite au non-respect de disposi-tions juridiques par rapport à des domaines de cette thématique et ce, soit par une action ou une omission de la part de la PME.

Une PME, quelle que soit sa taille, doit prendre conscience qu'elle peut être à tout moment confrontée à la cybercriminalité. Qu'il s'agisse, par exemple, de malveillances visant la destruction de données ou d'espionnage économique ou encore l'utilisation de son site web ou de ses ordinateurs et équipements comme relais pour l'attaque de site tiers.

Les conséquences des attaques informatiques pour les entreprises, sont généra-lement désastreuses et peuvent impacter leur pérennité. Chaque entreprise doit aujourd'hui se doter de mesures de sécurité inhérente à l'usage des nouvelles technologies.

Si les contraintes financières des petites structures restent un frein à la construc-tion d'une cybersécurité optimale, il existe des bonnes pratiques peu coûteuses et faciles à mettre en œuvre permettant de limiter une grande partie des risques liés à l'usage de l'informatique.

Le présent guide de cyber sécurité pour les PME marocaines, se veut simple est pratique. C'est le fruit d'une longue réflexion associant des professionnels aguer-ris et des académiciens de spécialités. Il constitue un moyen facile pour appliquer des règles et bonnes pratiques afin de protéger les outils informatiques et veiller à leurs pérennités. Le lecteur de ce guide n'a pas besoin d'être un expert de l'informatique ou du Web pour lire ou mettre en application les mesures qu'il propose. Certains termes propres à la cybersécurité sont utilisés, mais nous avons œuvré à les traduire en termes courant afin que tout lecteur puisse les utiliser. Ainsi, ce guide de bonnes pratiques a été élaboré afin de sensibiliser les PME sur cette problématique tout en leur apportant des moyens opérationnels à mettre en œuvre dans cette perspective et de devenir les acteurs de la sécurité de leurs entreprises.

Finalement, ce guide de sensibilisation basé sur une webographie et sur d'autres guides de cybersécurité internationaux, reste certainement non complet et ne peut dans aucun cas être considéré comme une référence dans un domaine as-sez vaste, tel celui de la Cyber-sécurité.

Les Petites et Moyennes Entreprises marocaines, comment faire face aux menaces cybernétiques ? Cette édition, améliorée et mise à jour l'AUSIM et le CMRPI, du guide de bonnes pratiques de cybersécurité des PME, guide élaboré dans le cadre de la Campagne Nationale de Lutte Contre la Cy-bercriminalité CNLCC 2014-2017, menée par le CMRPI et les partenaires institutionnels, sous l'égide du Ministère de l'Industrie, de l'Investissement, du Commerce et de l'Economie Numérique, fruit d'une collaboration et du tra-vail d'un comité de mise en place constitué, constitué en plus du Ministère parrain de la Campagne, des établissements et des organismes suivants :

- La Commission Nationale de Contrôle de la Protection des Données à Caractère Personnel - CNDP
- L'Agence Nationale de Réglementation des Télécommunications – ANRT
- La Confédération Générale des Entreprises du Maroc – CGEM
- Fédération Marocaine des Technologies de l'Information, des Télécom-munications et de l'Offshoring – APEBI
- Association des Utilisateurs des Systèmes d'Information au Maroc – AU-SIM
- Le Centre Marocain de Recherches Polytechniques et d'Innovation – CMRPI

## Menaces

## Cybercriminalité

# 1. RISQUES ET MENACES DE LA CYBERCRIMINALITE

## 1.1 Risque et impact de la cybercriminalité sur les PME

En 2015, Rex Mundi (« roi du monde » en latin), un groupe de pirates informa-tiques, plus précisément des cybercriminels, spécialisés dans le chantage sur internet, a publié sur internet un paquet de données personnelles qu'il s'est appropriées en pira-tant les sites de plusieurs entreprises. Avant de publier leurs données, il a exercé un chantage sur elles, en les menaçant de mettre l'information en ligne si elles ne lui payaient pas une somme considérable.

Cet exemple illustre une nouvelle fois que chaque entreprise connectée à inter-net est vulnérable. Il appartient donc à chaque entreprise, pour elle-même, mais aussi pour ses clients et fournisseurs, de se protéger contre la cybercriminalité et les cyber-risques. C'est toutefois plus vite dit que fait. Les cyberattaques sont de plus en plus complexes. De nouvelles formes de cybercriminalité se développent à toute vitesse. Une question fondamentale aussi évidente s'impose :

Les entreprises sont-elles suffisamment préparées face à ces risques nouveaux ?

Dans ce contexte, la lutte contre la cybercriminalité constitue une priorité pour les en-treprises afin d'assurer sa continuité et son développement dans un monde numérique interconnecté.

### 1.1.1 Cybersécurité

Une définition de la cybersécurité ainsi que l'ensemble des terminologies liées à cette notion sont données par la Recommandation X.1205 de l'Union Internationale des Télécommunications (UIT-T) comme suit :

La Cybersécurité est l'ensemble des outils, politiques, concepts de sécurité, mécanismes de sécurité, lignes directrices, méthodes de gestion des risques, actions, formations, bonnes pratiques, garanties et technologies qui peuvent être utilisés pour protéger le cyberenvironnement et les actifs des organisations et des utilisateurs.

Les actifs des organisations et des utilisateurs comprennent les dispositifs informatiques connectés, le personnel, l'infrastructure, les applications, les services, les systèmes de télécommunication, et la totalité des informations transmises et/ou stockées dans le cyberenvironnement.

La cybersécurité cherche alors à garantir que les propriétés de sécurité des actifs des organisations et des utilisateurs sont assurées et maintenues par rapport aux risques affectant la sécurité dans le cyberenvironnement.

Les objectifs généraux en matière de sécurité sont les suivants:

- **Confidentialité** : Objectif de sécurité permettant de s'assurer que les informations transmises ou stockés ne sont accessibles qu'aux personnes autorisées à en prendre connaissance.
- **Intégrité** : Objectif de sécurité qui consiste à empêcher, ou tout du moins à détec-ter, toute altération non autorisée de données. Par altération on entend toute mo-dification, suppression partielle ou insertion d'information. Cet objectif peut être assuré par la signature électronique.
- **Disponibilité** : Objectif de sécurité qui consiste à assurer un accès permanent à l'information et aux services offerts par le système d'information. C'est une garan-tie de la continuité de service et de performances des applications, du matériel et de l'environnement organisationnel.

### 1.1.2 Business

La cybercriminalité pourrait engendrer 3.000 milliards de dollars (2.200 milliards d'euros) de perte pour l'économie mondiale d'ici à 2002, selon le Forum économique mondial.

La cybersécurité est souvent perçue uniquement comme une réponse aux risques opé-rationnels. Mais c'est bien le risque systémique qui est le plus important car il est celui qui pèse sur l'avenir de l'entreprise qui, sans cybersécurité, ne parviendra pas à opé-rer sa transformation digitale dans de bonnes conditions.

Pour une entreprise le risque de la cybercriminalité est un risque de nature à impacter négativement sa croissance, sa capacité à conserver ou étendre sa position sur son marché, etc. Dans une étude récente Cisco établissait que les menaces informatiques étaient un frein à l'innovation des entreprises. En effet, même si celles-ci estiment que l'innovation est cruciale, nombreuses sont celles qui stoppent des projets de transfor-mation numérique innovants à cause de risques liés aux cyberattaques jugés trop im-portant.

### 1.1.3 Responsabilité

La cybersécurité d'une entreprise est une responsabilité partagée entre toutes ses composantes, surtout entre les ressources humaines du plus haut responsable au simple agent.

Les hauts dirigeants, les premiers responsables sur les activités de l'entreprise sont les plus sensés à veiller à la mise en place et au respect d'une politique de cybersécurité au sein de leurs entreprises. Ainsi ils doivent faire de la cybersécurité une priorité. La participation de la direction ou département sécurité des systèmes d'information est essentielle pour assurer une gestion rigoureuse de la cybersécurité. Les hauts diri-geants d'une organisation doivent communiquer l'importance de la sécurité et favori-ser une culture de sensibilisation à la sécurité. Ils doivent attirer l'attention sur la néces-sité d'être vigilant et de se tenir informé, et demander à leurs employés de réfléchir aux rensei-gnements personnels et professionnels qu'ils communiquent.

La direction ou le département responsable sur la sécurité des systèmes d'information, est responsable sur l'assurance du soutien pour la mise en place des mesures néces-saires à l'atténuation des risques de subir une attaque et des répercussions qui s'ensuivent. Considérant la quasi-certitude pour une organisation de subir une intrusion, ainsi que les coûts liés à la violation des données, l'investissement en matière de cy-bersécurité reste un prix bien modeste à payer contre les risques.

## 1.2 Essor de la menace

### 1.2.1 Caractère ludique, cupide, terroriste et stratégique

- **Caractère ludique** : Les nouvelles techniques de traitement de l'information (micro-ordinateurs, mo-dem...) ont créé cette menace, qui procède d'avantage, dans l'esprit de ceux qui en sont les auteurs, d'un jeu ou d'un loisir que d'un réel forfait (intrusion dans des systèmes, développement de virus ou de vers informatiques...). Animés d'un désir de s'amuser ou bien d'apprendre, ces auteurs possèdent généralement de bonnes connaissances techniques.

  Motivés par la recherche d'une prouesse technique valorisante destinée à démon-trer la fragilité du système plutôt que par souci de nuire, ils sont recrutés parmi les personnes soucieuses de s'affirmer, et ses victimes dans les organismes à forte no-toriété sur le plan technique ou réputés inviolables.

- **Caractère cupide** : Cette forme de délinquance, engendrée par l'apparition des procédés de trai-tement de l'information, et parfois dite en col blanc, peut avoir deux différents buts, parfois concomitants :
  - le premier se traduit par un gain pour l'attaquant ; ce gain peut être financier (détournement de fonds), lié à un savoir-faire (vol de brevet, concurrence dé-loyale...), ou de tout autre ordre ;
  - le second occasionne une perte pour la victime qui se traduira par un gain pour l'agresseur (parts de marché, accès au fichier des clients, à des propositions commerciales...) ; ce peut être la destruction de son système ou de ses informa-tions, une perte de crédibilité ou de prestige (image de marque) vis-à-vis d'une tierce personne, etc.

Il est difficile de caractériser, même succinctement, le profil type du fraudeur, tant les applications susceptibles d'être attaquées sont multiples. Néanmoins, les statis-tiques à ce sujet permettent de souligner que dans un grand nombre de cas, la menace a été initiée et mise en œuvre à l'intérieur même de l'organisme abritant le système et a été le fait d'employés, dont les antécédents ne permettaient pas de supposer qu'ils commettraient un forfait de ce type. Les victimes figurent en général parmi les organismes qui détiennent l'argent : banques, compagnies d'assurances, etc.

Pour sa part, le concurrent déloyal est plus facile à identifier : il figure parmi les concurrents, pour peu qu'ils soient parfaitement identifiés.

Nous ajouterons dans cette catégorie le crime organisé qui pourrait prendre de l'importance dans un futur proche s'il s'avère qu'il est plus facile - moins coûteux et moins risqué - de détourner les fonds de manière électronique qu'en pillant une banque.

- **Caractère terroriste** : On définira la menace terroriste comme regroupant toutes les actions concourant à déstabiliser l'ordre établi ; les actions entrant dans cette catégorie peuvent avoir un caractère violent (destruction physique de systèmes) ou plus insidieux (intoxica-tion et désinformation par détournement ou manipulation d'informations, sensibles ou non, perturbations engendrées dans un système et susceptibles de déclencher des troubles sociaux présents à l'état latent...).

  Mais leurs auteurs recherchent en général un résultat spectaculaire et les effets médiatiques qui l'accompagnent. Ce mode d'action relève de la manipulation et peut être l'une des expressions de la guerre psychologique.

  Les groupes, susceptibles de commettre ce genre de forfaits, disposent généralement de moyens financiers importants et de complicités au niveau international, leur permettant d'envisager pratiquement tous types d'attaque sur un système.

  Cette menace peut aussi être fomentée par un État qui veut mener une action de déstabilisation.

- **Caractère stratégique** : Pour un État, la menace stratégique s'intéresse par essence à toutes les informa-tions concernant le secret de Défense et la Sûreté de l'État, mais également à celles appartenant au patrimoine national, qu'il soit d'ordre scientifique, technique, industriel, économique ou diplomatique ; la menace stratégique, peut également attenter à la disponibilité de systèmes d'information, dont le fonctionnement continu est nécessaire au fonctionnement normal des institutions.

  Pour une entreprise ou une société, la menace d'origine stratégique aura pour but d'obtenir toute information sur les objectifs et le fonctionnement de celle-ci, pour récupérer des clients prospectés, des procédés de fabrication, des résultats de recherche et de développement et de porter atteinte à sa capacité de réaction. Elle sera principalement le fait de concurrents.

### 1.2.2 Les sources de risques

Les risques peuvent provenir principalement : de l'extérieur de l'entreprise (risques externes), de l'intérieur de l'entreprise (risques internes).

- **Risques externes**
  Les risques externes proviennent des changements ou des menaces dans l'environnement de l'entreprise (changements politiques, économiques, technologiques, sociologiques, changements dans les marchés, les clients, les concurrents, les produits, les fournisseurs) qui peuvent exercer une influence négative sur les objectifs et les stratégies de l'entreprise.

- **Risques internes**
  Les risques internes peuvent provenir de différentes sources : de la stratégie de l'entreprise, des processus, des ressources, des facteurs intangibles, de l'information de gestion.

- **Risques provenant de la stratégie**
  Les risques stratégiques peuvent être listés comme suit :
  - La stratégie n'est pas claire et précise
  - La stratégie n'a pas été communiquée adéquatement
  - La stratégie n'a pas été mise en œuvre adéquatement
  - La stratégie n'a pas été évaluée adéquatement

- **Risques provenant des processus**

  Les risques liés aux processus surviennent lorsque les processus ne sont pas performants. Les exemples suivants illustrent des risques découlant de processus non performants :

  - Le processus n'est pas aligné sur la stratégie de l'entreprise ;
  - Le processus ne donne pas satisfaction aux clients ;
  - Le processus n'opère pas de façon efficace et efficiente ;
  - Le processus a été modifié.

- **Risques provenant des ressources**

  - Changements dans les ressources humaines
  - Changements dans les ressources technologiques
  - Changements dans les ressources matérielles
  - Changements dans les ressources financières
  - Les ressources ne sont pas alignées sur la stratégie

- **Risques provenant des facteurs intangibles**

  - Changements dans la structure organisationnelle
  - Changements dans les conditions de performance
  - Changements dans les outils de gestion
  - Changements dans les compétences de gestion
  - Changements dans la satisfaction des parties prenantes
  - Les facteurs intangibles ne sont pas alignés sur la stratégie.

- **Risques provenant de l'information de gestion**

  L'information de gestion peut représenter aussi un risque lorsque l'information servant à prendre des décisions est incomplète, pas à jour, erronée, en retard, non pertinente, etc.

### 1.2.3 Témoignages sur la cybercriminalité : L'expérience de Sandra

Sandra travaille dans les ressources humaines à Miami, en Floride. Elle se sert d'un ordinateur dans le cadre de son travail depuis plus de dix ans. Au travail, son ordinateur est géré par le service informatique de l'entreprise et elle n'a jamais eu aucun problème de sécurité avec son ordinateur.

Elle ne se considère pas comme une néophyte en informatique et estime qu'elle ne risque pas vraiment d'être victime d'une fraude en ligne, pour les raisons suivantes :

- Elle n'achète rien en ligne car elle ne veut pas divulguer d'informations sur sa carte de crédit et ne veut pas que les informations concernant ses achats soient stockées et utilisées pour créer un profil de ses goûts.
- Elle utilise simplement son ordinateur domestique pour envoyer du courrier électronique à ses amis et à sa famille, pour consulter le Web à la recherche d'informations concernant son activité professionnelle et pour gérer ses comptes en ligne une fois par mois sur le site Web de sa banque.
- Il lui arrive occasionnellement de regarder d'autres choses sur Internet.

La situation de Sandra semble assez sûre.

Malheureusement, les apparences sont trompeuses. Au travail, elle a entendu parler d'une nouvelle vulnérabilité dans le navigateur Internet qu'elle utilisait. Le service informatique de son entreprise a dû appliquer un correctif d'urgence à tous les ordinateurs pour faire face à la situation.

Sandra voulait s'assurer que son ordinateur personnel était également protégé, elle est donc allée sur Internet dès qu'elle est rentrée chez elle pour chercher des informations sur cette vulnérabilité et pour vérifier si elle était protégée.

Grâce à un moteur de recherche connu, elle a trouvé un site Web qui proposait non seulement des informations sur cette vulnérabilité, mais aussi la possibilité de télécharger automatiquement un correctif adapté sur l'ordinateur. Sandra a lu toutes ces informations mais a refusé le téléchargement, car elle avait appris à refuser tout téléchargement en provenance d'une source suspecte. Elle a ensuite consulté le site officiel de son navigateur Internet pour obtenir le correctif. Quelle erreur a-t-elle commise ?

Malheureusement, alors que Sandra lisait des informations sur la vulnérabilité sur le premier site, l'escroc qui avait créé le site Web profitait du fait que son ordinateur était affecté de cette vulnérabilité. En fait, lorsqu'elle a cliqué sur Non (pour refuser le téléchargement proposé), un logiciel criminel petit mais puissant était déjà en train de s'installer à son insu.

Ce programme était un programme d'enregistrement de frappes de clavier. Au même moment, le créateur du site Web était déjà informé que le programme d'enregistrement de frappes de clavier s'était correctement (et secrètement) installé sur l'ordinateur de Sandra. Le programme était conçu pour enregistrer discrètement toutes les informations tapées à partir du clavier et pour les envoyer au créateur du site Web. Il a fonctionné

à merveille, enregistrant tout ce que Sandra tapait. Tous les sites Web visités, tous les messages électroniques envoyés étaient envoyés au cybercriminel.

Plus tard ce soir-là, Sandra a consulté son compte bancaire en ligne comme chaque mois. Lorsqu'elle s'est connectée pour consulter son compte bancaire personnel, le programme d'enregistrement de frappes de clavier a également enregistré ces frappes, y compris des informations confidentielles : le nom de sa banque, son identifiant d'utilisateur, son mot de passe, les quatre derniers chiffres de son numéro de sécurité sociale et le nom de jeune fille de sa mère. Le système de la banque était sécurisé et toutes les données saisies étaient chiffrées. Nul ne pouvait ainsi intercepter les informations. Cependant, le programme d'enregistrement de frappes de clavier enregistrait les informations en temps réel - pendant la frappe - avant qu'elles ne soient cryptées. Il était donc capable de contourner la sécurité qui avait été mise en place.

Ce n'était qu'une question de temps avant que le nom de sa banque, son identifiant d'utilisateur, son mot de passe et le nom de jeune fille de sa mère ne tombent aux mains du cybercriminel, qui a ajouté le nom et les données de Sandra à une longue liste d'utilisateurs peu méfiants. Il a ensuite vendu cette liste à une personne qu'il avait rencontrée sur Internet, spécialisée dans l'utilisation de données bancaires volées pour effectuer des retraits illégalement. Quelques semaines plus tard, lorsque Sandra est allée déposer de l'argent sur son compte, elle a été étonnée de constater que son compte était presque vide. Sandra a été la victime d'un cybercrime.

Gouvernance

Cybersécurité

# 2. GOUVERNANCE DE LA CYBERSECURITE

## 2.1 Gestion de la cybersécurité

### 2.1.1 Politique de sécurité des SI

Suite à l'évaluation des risques, un plan de sécurité doit être dressé. Ce plan peut reprendre les actions suivantes :

- Faire le recensement des biens de l'entreprise
- Faire un plan d'action pour améliorer la sécurité SI (mesures de sécurité et décisions)

Ce plan doit être mis à jour au fur et à mesure des réalisations et de la revue des risques ou bien au moins une fois par année.

L'entreprise devrait inclure les dépenses relatives à la sécurité SI dans le budget général de l'entreprise vu le cout financier de certaines mesures.

On peut noter aussi qu'une grande partie des mesures peuvent être gratuites ou avec des couts bas.

Dans certains cas, il faut étudier l'opportunité de souscrire à des assurances pour couvrir les risques sécurité SI.

### 2.1.2 Charte d'usage des SI

Une charte de bon usage des systèmes d'Information au sein d'une entreprise définit les règles d'usages de l'ensemble des moyens matériels, logiciels, applications, bases de données, réseaux de télécommunications et informatique (clé USB, ordinateur portable, téléphone mobile, etc.). Elle précise également les droits et devoirs de chaque utilisateur afin d'assurer la sécurité du système d'information et la protection des utilisateurs.

La charte responsabilise l'utilisateur de l'usage qu'il fait du système d'information auquel il a accès ; il est soumis au respect des obligations résultant de son statut ou de son contrat.

Une charte de bon usage des SI, doit fixer l'ensemble des bonnes pratiques de cybersécurité au sein de l'entreprise, traduisant la politique de sécurité des SI adoptée.

### 2.1.3 Gouvernance des SI et aspect organisationnel

Comme toute entreprise, les PME doivent veiller à la gestion de leurs Systèmes d'Information qu'ils soient géré en interne ou externalisé. La pierre angulaire de ce système reste la sécurité SI ou la cybersécurité.

Chaque entreprise doit désigner un collaborateur pour la gestion de la sécurité SI même si ce dernier a d'autres taches en parallèle.

La personne en charge de la SSI doit assurer les points suivants :

- Planifier et exécuter les mesures de sécurité SI
- Accompagner les autres employés en matière de sécurité SI
- Exécuter et maintenir les politiques et chartes internes de sécurités SI

La direction de l'entreprise devrait :

- Appuyer les projets et le responsable de Sécurité SI
- Faire rédiger et valider une politique de sécurité SI
- Donner de l'importance à la sécurité et inciter les employés au respect de la politique SSI
- Etablir un plan de sécurité ou/et une politique de sécurité

Une politique de sécurité est un document qui décrit l'organisation de la sécurité SI au niveau de l'entreprise, et les droits et obligations du personnel vis-à-vis de la sécurité SI. Ce document peut être composé seulement de deux ou trois pages.

### 2.1.4 Le besoin en sécurité du SI

La sécurité du SI fait appel à des solutions techniques, mais également à la mise en place rigoureuse d'une organisation adaptée aux objectifs recherchés. Cela passe par des mesures de sensibilisation, de formation des utilisateurs, ainsi que par l'expression de règles clairement définies.

La SSI c'est donc la sécurité du système informatique mais aussi la prise en charge des aspects patrimoniaux du SI, notamment afin que les utilisateurs puissent utiliser le SI en toute confiance.

Le besoin de maintenir l'intégrité de l'information et de protéger les actifs informatiques exige un processus de gestion de la sécurité. Ce processus comporte la mise en place (et la maintenance) de rôles et de responsabilités, de politiques, de plans et procédures informatiques.

### 2.1.5 Sensibilisation à la cybersécurité

Etant donné que l'humain constitue une source de défaillance dans la sécurité des SI au sein d'une PME. Les PME doivent sensibiliser les employés à la sécurité SI et vulgariser le vocabulaire et les pratiques sécuritaires.

Il faut établir un programme de sensibilisation à la sécurité SI qui est destiné à tous les employés de l'entreprise.

Ce programme devrait proposer une formation de base sur la sécurité SI en plus des pratiques à adopter lors de l'exercice des fonctions.

- Le programme peut être simple et facile à mettre en œuvre.
- La sensibilisation peut se faire via plusieurs canaux (formation, mail, affichage…).

Il est indispensable de mettre des moyens technologiques pour sécuriser le système d'information, mais tout ce travail dans ce sens est conditionné par le comportement humain. La plupart des vulnérabilités et des attaques récentes exploitent des failles humaines de comportement et de manque de vigilance ou tout simplement d'ignorance.

A cet effet, l'employé de la PME devrait observer les consignes suivantes :

- Vérifier l'existence d'un antivirus mis à jour sur le poste de travail
- Planifier des analyses périodiques du système
- Choisir un mot de passe complexe, difficile à deviner (majuscules, minuscule, chiffres, lettre, caractères spéciaux, etc.)
- Ne pas écrire le mot de passe sur un support papier à proximité du poste de travail, faire attention à la composition de son mot de passe et à la conservation de celui-ci
- Ne jamais divulguer le mot de passe ou le nom d'utilisateur
- Changer le mot de passe régulièrement
- Protéger les fichiers sensibles par un mot de passe, chiffrement, etc.
- Maintenir le bureau clair de tout document confidentiel
- Désactiver le WIFI sauf durant son usage
- Sauvegarder les données critiques
- Eviter l'installation par soi-même de logiciels sur le poste de travail
- Etre vigilant par rapport aux mails reçus dont on ignore la provenance ou l'expéditeur. Les supprimer et réclamer au helpdesk
- Ne pas divulguer les informations propres à la société
- Faire attention aux sites web suspects et ne pas cliquer sur les liens inconnus
- Faire attention à sécuriser vos appareils mobiles au même niveau que les autres appareils informatiques
- Etre vigilant lors de l'utilisation de services sensibles tels que la banque en ligne …
- Séparer l'utilisation professionnelle de l'utilisation personnelle

## 2.2 Normes et standards de la cybersécurité

Une norme désigne un ensemble de spécifications décrivant un principe servant de référence technique.

Les normes et standards permettent :

- De fournir un guide et une terminologie commune (prescriptive ou directive)
- D'indiquer les voies d'amélioration et de mesurer le trajet accompli (modèles de maturité)
- D'apporter un cadre de référence partagé aux audits

A la fin des années 1990, le British Standard Institution publie un document qui précise les exigences de mise en œuvre d'un système de management de la sécurité de l'information (SMSI). Aujourd'hui ce document est devenu la série des normes ISO 27000 (Fig 1). Il repose sur un ensemble de définitions, de recommandations, d'exigences de sécurité. Ces normes sont applicables au système d'information de la sécurité et à certains domaines spécifiques. Le SMSI apporte les garanties sur la capacité de l'entreprise à maîtriser les coûts et les priorités en matière d'investissements et d'orientations budgétaires au regard des enjeux business et des risques de sécurité

Les points couverts par la série des normes ISO 27000 sont notamment :

- Gouvernance
- Politiques et directives
- Architecture et standards
- Surveillance et conformité
- Définition et implémentation des systèmes
- Définition et implémentation des technologies
- Opérations
- Sensibilisation
- Gestion du risque
- Surveillance et conformité
- Périmètre stratégique
- Périmètre opérationnel

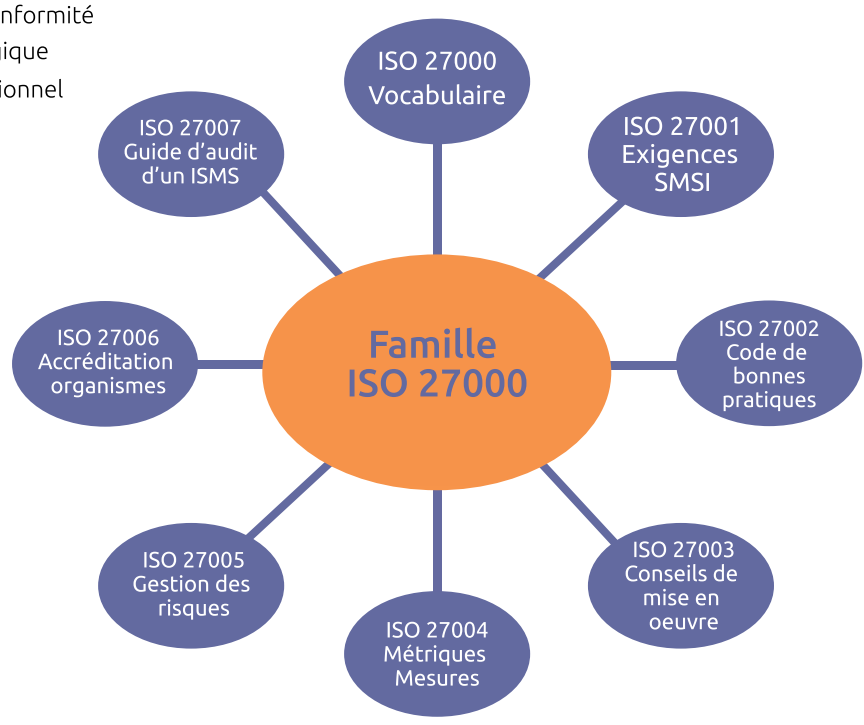



Fig 1 : schéma de la famille des normes ISO 27000

## 2.3 Norme ISO-27002 : ensemble de mesure de sécurité

La norme ISO/IEC 27002 recense de nombreux objectifs de contrôle répartis dans chacun des onze domaines suivants :

- Politique de sécurité
- Organisation de la sécurité
- Gestion des actifs
- Sécurité du personnel
- Sécurité physique et sécurité de l'environnement
- Gestion des opérations et des communications
- Contrôle d'accès
- Gestion des incidents de sécurité
- Acquisition, développement et maintenance des systèmes d'information
- Gestion de la continuité d'activité
- Conformité

Les objectifs de contrôle sont des principes généraux pouvant servir de base à la politique de sécurité.

- Aucun contrôle n'est obligatoire : si une organisation choisit de ne pas mettre en place un contrôle ou de ne pas respecter un objectif de contrôle, elle doit justifier que cette décision découle d'un processus rationnel et argumenté.
- L'entreprise choisit les contrôles requis identifiés après une analyse de risques appropriée.
- Elle peut également adopter des contrôles non recensés dans le standard pour couvrir un risque particulier.

## 2.4 Norme ISO-27001 : Système de Management des SI

La norme internationale ISO 27001 spécifie un Système de Gestion de la Sécurité de l'Information (SGSI) qui est aussi appelé Système de Management de la Sécurité d'Information (SMSI).

Ce SMSI est structuré en quatre étapes récurrentes : planifier, mettre en œuvre, vérifier et améliorer, afin de respecter le principe de la roue de Deming, issue du monde de la qualité. Ces étapes sont largement connues sous l'intitulé en anglais ''PDCA'' (Plan, Do, Check and Act).

Ce concept permet d'établir un parallèle avec les normes relatives aux systèmes de management de la qualité (ISO 9001) et de l'environnement (ISO 14001).

1. **Planifier** (établissement du SMSI)

   Etablir la politique, les objectifs, les processus et les procédures du SMSI relatives à la gestion du risque et à l'amélioration de la sécurité de l'information de manière à fournir des résultats conformément aux politiques et aux objectifs globaux de l'organisme.

2. **Déployer et mettre en œuvre** (fonctionnement du SMSI)

   Mettre en œuvre et exploiter la politique, les mesures, les processus et les procédures du SMSI.

3. **Contrôler/vérifier** (vérifier et réexamen du SMSI)

   Evaluer et, le cas échéant, mesurer les performances des processus par rapport à la politique, aux objectifs et l'expérience pratique et rendre compte des résultats à la direction pour réexamen.

**4. Agir/améliorer** (mise à jour du SMSI)

Entreprendre les actions correctives et préventives, sur la base des résultats de l'audit interne du SMSI et de la revue de direction, ou d'autres informations pertinentes, pour une amélioration continue dudit système.

En résumé, ISO 27001 introduit deux concepts clés :

- Une approche de la sécurité fondée sur les risques (on ne met en œuvre que ce qui est nécessaire),
- La gouvernance de la sécurité : la sécurité n'est pas réduite à une question technologique, mais elle exige un bon modèle de personnel-processus mais elle exige un bon modèle de gouvernance et comprend la responsabilisation ("accountability") et des processus de décision engageant le ''top management'' de l'entreprise.

La norme 27001 impose l'établissement d'un système de gestion de la sécurité de l'information (SGSI ou SMSI), décrit dans un cadre de gestion.

- Les objectifs et mesures de contrôle doivent être mis en œuvre et documentés.
- La documentation doit être contrôlée.
- Des registres matérialisant les contrôles doivent être maintenus

## 2.5 Norme ISO-27005 : gestion des risques des SI

La norme ISO 27005 , norme internationale concernant la Sécurité de l'information publiée conjointement par l'Organisation Internationale de Normalisation (ISO) et la Commission Electrotechnique Internationale (CEI). Il s'agit un recueil de lignes directrices traitant spécifiquement de la gestion des risques dans le contexte de la Sécurité des Systèmes d'Information. Elle définit le capital à protéger concernant la sécurité de l'information à savoir :

- Les actifs primaires :
  - Les processus et l'activité
  - L'information
- Les actifs de support :
  - Le matériel
  - Les logiciels
  - Les réseaux
  - Le personnel
  - Les sites
  - Le support organisationnel (autorités de tutelle, maison-mère, département)

## Aspect juridique


## Conventionnel

## 2.6 Aspect juridique et conventionnel

La Cybersécurité pour les entreprises : protection de la concurrence et de la malveillance leur système d'information qui irrigue l'ensemble de leur patrimoine (propriété intellectuelle et savoir-faire) et porte leur stratégie développement.

La sécurité vise généralement les objectifs de : confidentialité, intégrité, disponi-bilité, authentification, non répudiation … et de plus en plus la conformité à un régime juridique.

Le Maroc dispose d'un cadre juridique traduit par de textes de lois s'alignant avec l'ensemble des conventions internationales ratifiées, ainsi et en particulier on peut citer les lois : 07-03, 53-05, 31-08, 09-08,17-97 et la directive DNSSI. (Fig 2).

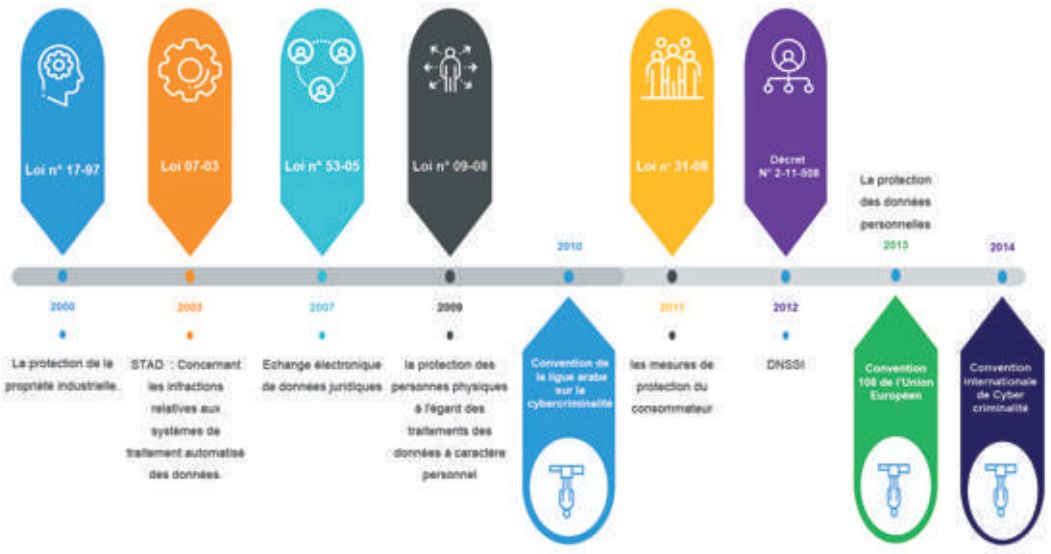



Fig 2. Historique de l'arsenal juridique au Maroc

### 2.6.1 Loi 07-03

Concernant les infractions relatives aux systèmes de traitement automatisé des don-nées (STAD). Cette loi complétant le code pénal en ce qui concerne les infractions re-latives aux systèmes de traitement automatisé des données (2003).

### 2.6.2 Loi n° 53-05

En Relation avec l'échange électronique de données juridiques. Cette loi sur l'échange électronique (2007) sanctionnant notamment les fraudes liées aux moyens de preuves électroniques ainsi que le recours à la cryptographie non autorisé et/ou pour des fins nuisibles).

### 2.6.3 Loi n° 31-08

En relation avec les mesures de protection du consommateur Elle définit les droits et les obligations ainsi que les règles générales qui s'appliquent aux commerçants qui fournissent des biens ou des services aux consommateurs, et des règles particulières à certains types de biens ou de services, Le e-commerce ou encore le commerce électro-nique n'échappe pas à ses règles. Ainsi la loi prévoit certaines dispositions visant à protéger les consommateurs. (publiée au bulletin officiel n°5932 du 7 avril 2011).

### 2.6.4 Loi n° 09-08

En relation avec la protection des personnes physiques à l'égard des traitements des données à caractère personnel. Cette loi sur les données personnelles (2009) sanc-tionnant pénalement les atteintes aux données personnelles (prévoyant des obliga-tions spécifiques en matière de sécurité, confidentialité et sous-traitance des données à caractère personnel.).

### 2.6.5 Loi n° 17-97

En relation avec la protection de la propriété industrielle telle qu'elle a été modifiée et complétée. (Promulguée par Dahir n° 1-00-91 du 9 Kaada 1420 (15 février 2000)).

### 2.6.6 Contrat de sous-traitance

Due principalement aux besoins des entreprises en machines puissantes, mais aussi peu volumineuses, la sous-traitance de spécialité est un moyen pour les entreprises de maîtriser et de limiter leurs dépenses informatiques.

Les risques assumés par les entreprises de sous-traitance sont souvent considérables et impliquent une couverture solide par une assurance adaptée. De plus, ce contrat con-duit souvent à un transfert de « données personnelles » du client ; données protégées et donc soumises aux contraintes de la loi 09-08.

La sous-traitance est organisée par voie contractuelle, comportant parfois un contrat-cadre assorti de contrats d'application. En principe un tel contrat doit être définit les modalités d'exécution du contrat et la nature des obligations.

### 2.6.7 Infogérance et externalisation des SI

L'infogérance consiste, pour une entreprise, à confier à un prestataire extérieur le soin d'héberger, gérer et maintenir un système d'Information ou une application permet-tant d'assurer tout ou partie des traitements de données dont elle a besoin.

Les différentes prestations d'infogérance peuvent êtres alors globale, partielle, d'exploitation ou d'application).

### 2.6.8 Convention internationale de Cybercriminalité

La Convention sur la cybercriminalité, faite à Budapest le 23 novembre 2001 et du Protocole additionnel à ladite Convention, fait à Strasbourg le 28 janvier 2003 (pu-blication au BO N°6262 du 5 juin 2014).

### 2.6.9 Convention 108 de l'Union Européen

La protection des données personnelles a été garantie pour la première fois - en tant que droit distinct accordé à un individu - dans la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel (Convention 108). Cette dernière a été adoptée par le Conseil de l'Europe en 1981, par le gouvernement marocain le 06 juin 2013.

### 2.6.10 Convention de la ligue arabe sur la cybercriminalité

Convention arabe contre la cybercriminalité signée par le Maroc le 21 décembre 2010, cette convention vise à renforcer la coopération entre les pays arabes dans ce domaine, afin de pouvoir faire face aux conséquences néfastes de ce type de crimi-nalité sur la sécurité et les intérêts de ces Etats et de leurs sociétés nationales.

### 2.6.11 la Directive Nationale de la Sécurité des Systèmes d'Information DNSSI

Face à la montée en puissance des vulnérabilités des systèmes d'information et à la recrudescence des cy-berattaques, le Comité Stratégique de la Sécurité des Systèmes d'Information (CSSSI) institué par le décret n° 2-11-508 du 21 septembre 2011 a adopté en date du 05 décembre 2012 la stratégie nationale de la cyber sécurité.

## Organismes concernés :

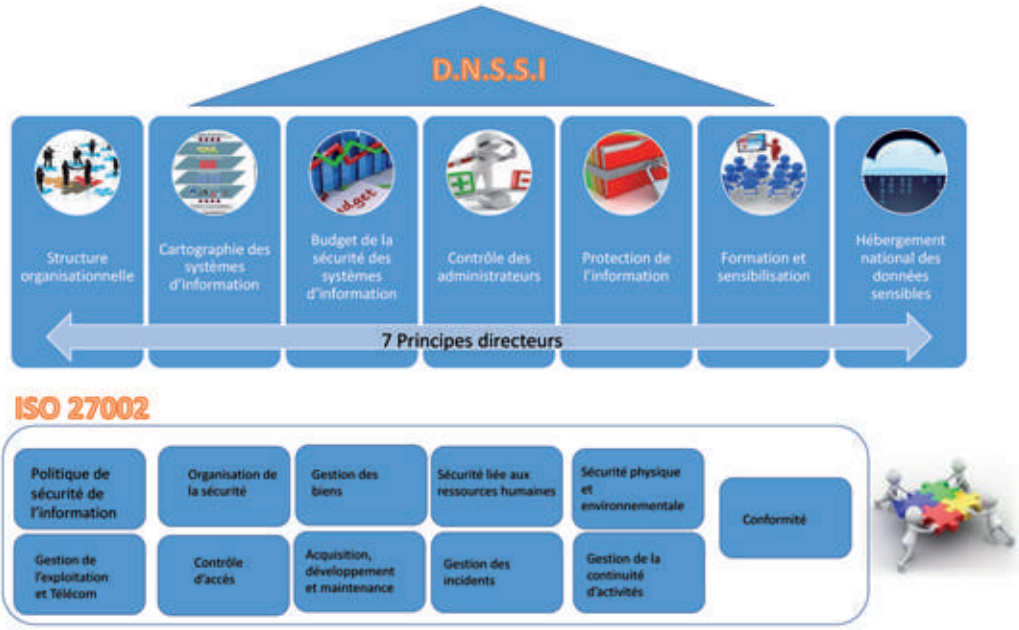
Ce dernier (CSSI) a approuvé un plan d'actions qui consiste à élaborer et mettre en oeuvre une Directive Nationale de la Sécurité des Systèmes d'Information (DNSSI) avec pour objectifs d'élever et d'homogénéiser le niveau de protection et le niveau de maturité de la sécurité de l'ensemble des sys-tèmes d'information des administrations et organismes publics ainsi que des infrastructures d'importance vitale.

Pour arrêter les règles de la DNSSI, la DGSSI s'est inspirée de la norme marocaine NM ISO/CEI27002:2009 et s'est basée sur les résultats de l'enquête menée au mois de juillet 2013 auprès d'un échantillon représen-tatif d'administrations et organismes publics et d'opérateurs d'importance vitale.
La DGSSI met à la disposition de chaque entité un tableau de bord pour le suivi de l'application de la DNSSI ainsi que les guides techniques d'implémentation des différentes règles de sécurité.

Chaque entité élabore son bilan annuel de mise en application de la DNSSI en se basant sur ledit tableau de bord, et le soumet annuellement à la DGSSI qui consolidera une synthèse servant à la prise de décision du CSSSI, notamment pour arrêter le périmètre des audits à effectuer par la DGSSI.

## Principes directeurs :

La DNSSI s'appuie sur sept principes directeurs, issus de la Stratégie Nationale de la cyber sécurité, basés sur onze règles inspirées de la norme ISO 27002.




## Objectifs et règles :

Les entités doivent implémenter les règles selon un classement de sensibilité A, B ou C de leurs Systèmes d'information sur lesquels une atteinte à la confidentialité, à l'intégrité ou à la disponibilité peut entraîner un impact sur leur capacité à remplir les missions vitales pour la nation dont elles sont chargées, sur leurs biens essentiels, ou sur leurs individus.

A chaque règle est associé :

- Un poids allant de 1 à 4 et qui traduit le niveau d'impact croissant de son non-respect sur le SI en termes de disponibilité, d'intégrité, de confidentialité ou de de traçabilité;
- Le(s)responsable(s) concerné(s)devant veiller à l'implémenter et/ou la faire respecter notamment la Direction Générale, le Secrétariat général, la Direction SI, RSSI….etc.).

### Réflexions à mener :

Cette directive concerne directement les systèmes d'information des administrations et organismes publics ainsi que des infrastructures d'importance vitale, mais ça n'empêche que les partenaires et les prestataires de ces organismes soient au même niveau de maturité de sécurité pour travailler dans un cadre cohérent…

## 2.6.12 Autres règlements qui peuvent impacter le paysage de la sécurité :RGPD

Le nouveau Règlement européen sur la protection des données personnelles appelé en français RGPD « Règlement général sur la protection des données » ou en anglais GDPR « General Data Protection Regulation » vise à renforcer la sécurité des données personnelles des citoyens européens en Europe mais aussi en dehors de l'Europe. Tout organisme public ou privé utilise ou stocke une donnée personnelle d'un citoyen européen, est amené à respecter le RGPD. Ce règlement est une évolution naturelle de tous les textes existants dans les pays européens afin que le citoyen garde la main sur ses données personnelles quelque soit le lieu, le pays ou l'origine de l'entreprise qui les stockent. Cela vient aussi répondre aux différentes craintes des géants des réseaux sociaux sur internet (entre autres) qui peuvent utiliser des données sans consentement expresse de l'utilisateur en question.

Cela concerne aussi les sous-traitants.

Le règlement est entré en vigueur depuis le 25 Mai 2018. Cela implique que tous les traitements qui sont appliqués doivent se conformer aux nouvelles directives. Les sanctions sont progressives pouvant aller jusqu'à 20 millions d'euros pour une administration et jusqu'à 4% du CA annuel mondial pour une entreprise.

Une ventilation de la mise en place du règlement 7 étapes :

**1- Organisation et gouvernance** : Nommer un DPO « Data Protection Officer », créer une organisation cible, créer des instances de suivi et des procédures pour un suivi rigoureux des traitements

**2- Traitements** : Cartographier les traitements, mettre en place un registre des traitements, préparer des fiches de traitements et mener des contrôles internes

**3- Protection** : Gérer les contrôles d'accès aux données à caractère personnel, gérer la sauvegarde et la restauration, mettre en place des procédures de droits d'accès, de minimisation et anonymisation, de chiffrement des mails, de chiffrement des PCs, de la rétention des données et de résilience du Système d'information

**4- Droits** : Mettre en place une procédure de traitement des demandes, de gestion des droits et de droits à l'oubli

**5- Violations** : mettre en place une procédure de notification des violations, sensibiliser le personnel des violations, les intégrer aux contrats, identifier les personnes impactées

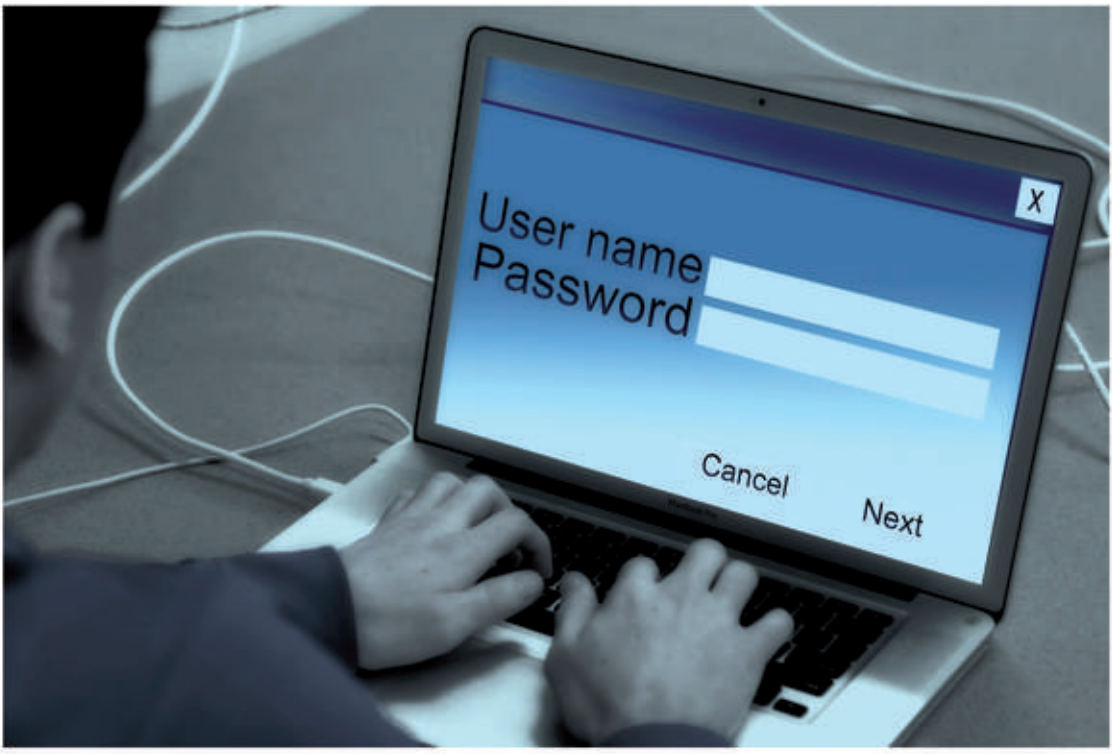
**6- Sous-traitants** : Identifier les sous-traitants, revoir les contrats de sous-traitance, intégrer les obligations RGPD aux contrats, mettre en place une produre de Droits à l'oubli « suppression des données personnelles »

**7- Projets** : Mener une analyse d'impact sur les données personnelles (PIA), Rédiger une procédure « Privacy by design » et « Privacy by default » et les mettre en place.

## Quelques recommandations pour la loi 09-08. :

- La loi 09-08 prévoit la demande des autorisations et la déclaration des traitements pour lesquels le responsable du traitement (RT) reçoit un récépissé, dans le cadre du RGPD, les RT seront dans une logique continue de mise en conformité pour l'ensemble des traitements.
- Le RGPD est venu apporter plus de clarté et de sécurité aux données personnelles des citoyens européens. Il oblige la notification des incidents remontés sur la protection des données à l'autorité compétente.
- En quelque sorte, le RGPD vient confirmer la portée de la loi marocaine tout en l'amenant à transiter du régime déclaratif à un régime de mise en conformité continu.
- La loi 09-08 peut s'inspirer du règlement européen afin de compléter le dispositif national
- La loi 09-08 doit penser à son évolution afin de suivre la digitalisation des organismes publics et privés ainsi que les données personnelles des citoyens marocains
- La loi 09-08 doit penser à protéger les données personnelles des citoyens marocains au niveau mondial pour contrecarrer les grands du Net
- Le Maroc doit créer une alliance au niveau africain pour qu'un règlement non marocain mais africain voit le jour pour lui donner la force de force dont il aura besoin au niveau mondial

## Protection




## Mesures

# 3. MESURES DE PROTECTION CONTRE LA CYBERCRIMINALITE

## 3.1 Sécurité du poste de travail et des serveurs Rôle de l'Antivirus

### 3.1.1 Sécurité du poste de travail

- Ne pas installer des logiciels sur le poste de travail
- Eviter la modification de la configuration du poste de travail
- Faire des sauvegardes régulières des documents importants
- Paramétrer un écran de verrouillage : ne pas laisser le poste de travail accessible avec la session ouverte

### 3.1.2 Les virus, antivirus et firewall

- Ne jamais copier sur le poste de travail des fichiers provenant de sources douteuses (USB, email, etc.)
- Signaler tout incident d'infection de virus
- En cas d'infection ; déconnecter le poste de travail du réseau local

### 3.1.3 Sécurité des serveurs

La politique de sécurité doit englober l'ensemble du réseau informatique. La plupart des tentatives d'intrusions peuvent provenir (volontairement ou non) des utilisateurs autorisés. Pour cela, les mesures de sécurité doivent prendre en considération le réseau local, appelé LAN (Local Area Network), et le réseau externe connu sous le nom WAN (Wide Area Network).

### 3.1.4 L'authentification des utilisateurs

Le premier niveau de sécurité à prendre en compte dans un LAN est l'utilisateur. Pour accéder aux ressources locales et réseaux, il devra s'identifier grâce à un nom d'utilisateur et à un mot de passe. Chaque utilisateur doit être unique dans son contexte et appartenir à au moins un groupe d'utilisateurs. Certaines règles sont à respecter :

- Le nom d'utilisateur (Login) doit être significatif pour pouvoir identifier toutes les personnes. Plusieurs méthodes d'identification sont possibles. L'une d'entre elles consiste à associer la première lettre du prénom au nom complet de la personne. Par exemple, le nom d'utilisateur "rchbeir" est utilisé par l'utilisateur Richard CHBEIR. Par ailleurs, chaque système d'exploitation propose des comptes administrateurs (admin sous Novell, root sous Unix, et administrator sous Windows) capable de gérer les utilisateurs (création, attribution des droits et des fichiers, etc.).
- Le mot de passe (Password) doit être personnel et incessible. Certaines consignes peuvent rendre difficiles voire inefficaces les tentatives de connexion des pirates
- Le mot de passe doit contenir au moins 8 caractères dont 2 numériques
- Le renouvellement périodique (mensuel si possible) du mot de passe
- Le cryptage des données pour rendre l'interception et la surveillance moins efficaces
- La déconnexion et le blocage du système après un certain nombre de tentatives de connexion
- L'interdiction de se connecter avec des comptes administrateurs sur des postes non sécurisés

### 3.1.5 Les permissions d'accès

Afin de rendre votre politique de sécurité plus efficace, il faut établir convenablement les droits d'accès des utilisateurs et des groupes. L'installation standard des systèmes d'exploitation (Unix, Windows NT, Novell, etc.) n'est pas sécurisée en soi. Elle nécessite certaines manipulations. Quelques points fondamentaux cités ci-dessous peuvent apporter un niveau minimal de sécurité :

Sécurité des fichiers contenant les mots de passe : sous les systèmes Unix, deux fichiers sont à prendre en compte : le fichier des utilisateurs et leurs mots de passe : "/etc/passwd", et celui des groupes : "/etc/groups". Les deux fichiers cryptés sont accessibles à tous les utilisateurs, même "guest" ou "anonyme", sans quoi ces derniers ne pourraient pas se connecter. Ce qui les rend, malgré le cryptage, faciles à pirater. En effet, certains outils permettent de les décrypter. Pour remédier à cela, l'administrateur (root) peut exécuter la commande "shadow" permettant de transférer le contenu de ces deux fichiers dans un autre fichier inaccessible aux utilisateurs. D'autre part, sous Windows, la base de registre contenant les paramètres cryptés du système (system.dat) et des utilisateurs (user.dat) doit être protégée. Microsoft propose deux outils : "poledit" et "regedit" qui permettent de manipuler et de personnaliser entièrement le système. A l'aide de ces deux outils, vous pouvez minimiser les risques d'intrusions :

En interdisant l'exécution de l'Explorateur Windows, des commandes MS-DOS et les outils de la base de registre (Poledit et regedit).

En autorisant l'exécution d'une liste d'applications comme Winword, Excel, etc.

En interdisant les modifications des paramètres de configuration (panneau de configuration, imprimante, etc.).

Attribution convenable des droits d'accès : dans un LAN, chaque utilisateur doit pouvoir créer et gérer des fichiers et des répertoires dans son espace de travail. Les autorisations d'accès (lecture, écriture, listage, exécution, etc.) aux fichiers et programmes doivent être parfaitement étudiées et installées. Dans une politique standard de sécurité, un simple utilisateur possède, d'une part, son répertoire de travail où il a tous les droits d'accès, et, d'autre part, des répertoires plus restreints appropriés à son activité. Il faut en principe éviter de donner le droit d'installation des programmes, de sauvegarde des fichiers système, de création de compte, d'ouverture des sessions sur le terminal du serveur, aux utilisateurs non autorisés.

### 3.1.6 Sécurité de l'accès à distance

VPN : (Virtual Private Network ou réseau privé virtuel ou RPV), ensemble de réseaux qui apportent des services de sécurité complémentaires à ceux offerts par les firewalls.

Les VPN est une garantie de l'intégrité et la confidentialité des données échangées entre sites distants via Internet ou des réseaux publics non sécurisés.

L'emploi d'ordinateurs portables, d'ordiphones (smartphones) ou de tablettes facilite les déplacements professionnels ainsi que le transport et l'échange de données. Voyager avec ces appareils nomades fait cependant peser des menaces sur des informations sensibles dont le vol ou la perte auraient des conséquences importantes sur les activités de l'organisation. Il convient d'appliquer les règles suivantes :

- Eviter les connexions Wifi gratuites
- Utilisez de préférence du matériel dédié aux missions (ordinateurs, ordiphones, supports amovibles tels que les disques durs et clés USB)
- Imposer un mot de passe au démarrage de la machine (mot de passe de « boot »)
- Instaurer un verrouillage automatique de la session après un certain délai d'inactivité, et prévoir un mot de passe alphanumérique complexe (chiffres + lettres + caractères spéciaux) pour le déverrouillage
- Désactiver les fonctions de communication wifi et Bluetooth de vos appareils nomades
- Mettre en œuvre une solution de chiffrement des données
- Sauvegarder les données que vous emportez et laissez la sauvegarde en lieu sûr
- Éviter de partir avec des données sensibles
- Marquer vos appareils d'un signe distinctif (comme une pastille de couleur)
- Garder vos appareils, support et fichiers avec vous

- Protéger l'accès de vos appareils par des mots de passe forts
- Ne vous séparez pas de vos équipements
- Utiliser un logiciel de chiffrement pendant le voyage
- Effacer l'historique de vos appels et de vos navigations
- En cas de perte ou de vol d'un équipement ou d'informations, informer immédiatement votre organisme
- Ne pas utiliser les équipements qui vous sont offerts (clés USB). Ils peuvent contenir des logiciels malveillants
- Ne pas connecter vos équipements à des postes ou des périphériques informatiques qui ne sont pas de confiance
- Changer tous les mots de passe utilisés pendant le voyage

### 3.1.7 Politique de mise à jour des systèmes d'exploitation et logiciels

Dans chaque système d'exploitation (Android, IOS, MacOS, Linux, Windows,…), logiciel ou application, des vulnérabilités existent. Une fois découvertes, elles sont corrigées par les éditeurs qui proposent alors aux utilisateurs des mises à jour de sécurité. Les attaquants exploitent ces vulnérabilités pour mener à bien leurs opérations encore longtemps après leur découverte et leur correction.

Il convient donc, au sein de l'entreprise, de mettre en place certaines règles :

- S'il existe un service informatique au sein de l'entreprise, il est chargé de la mise à jour du système d'exploitation et des logiciels
- S'il n'en existe pas, il appartient aux utilisateurs de faire cette démarche, sous l'autorité du chef d'entreprise
- Configurez vos logiciels pour que les mises à jour de sécurité s'installent automatiquement chaque fois que cela est possible. Sinon, téléchargez les correctifs de sécurité disponibles
- Utilisez exclusivement les sites Internet officiels des éditeurs

## 3.2 La sécurité WEB

### 3.2.1 Règles d'utilisation de l'internet

L'accès internet s'est démocratisé au-delà du lieu de travail. Il est possible depuis le mobile, chez soi, et même dans les lieux publics à travers les réseaux mobiles et wifi. Il est important que le collaborateur prenne conscience de l'importance de se prémunir contre la fuite d'informations sur le web.

Très utile en entreprise, le web peut constituer un risque, si le collaborateur y divulgue des informations personnelles ou professionnelles, sciemment ou insciemment.

Pour cela il est important de faire comprendre aux collaborateurs les simples mesures de sécurité suivantes :

- Vérifiez constamment la légitimité des sites web que vous visitez, et surtout lorsque vous êtes amenés à y partager des renseignements personnels
- Lorsque vous renseignez un formulaire avec des informations sensibles, assurez-vous que vous utilisez un poste de travail sécurisé, et que le site web en question est sécurisé (mention https sur l'adresse, et verrou en icône sur le navigateur).
- Si vous recevez un email avec un lien vers un site web, méfiez-vous. Les emails à consonance commerciale ou lucrative (appelant à se faire reconnaitre pour un gain quelconque), sont souvent des tentatives de « fishing ». Supprimez l'email et contactez l'administrateur
- N'enlevez ou ne désactivez jamais les mesures de protection mises en place dans les réseaux et les ordinateurs de l'entreprise (comme l'antivirus ou le parefeu)

- Installez une extension de votre navigateur pour classifier la réputation du site que vous visitez, des extensions existent pour l'ensemble des navigateurs permettant de rajouter une protection en vous informant sur le degré de danger du site en question

L'utilisateur ne doit pas :

- Utiliser des moyens de connexion autre que ceux offerts par votre organisme (4G, etc.)
- Télécharger de fichier depuis des sites douteux
- Utiliser les postes de travail ou l'identité d'autres personne pour naviguer l'internet
- Naviguer sur des sites douteux ou à caractère immoral
- Effectuer de téléchargements illégaux
- Divulguer sur Internet des informations à caractère confidentiel ou pouvant porter préjudice à l'organisme
- Abuser de la navigation sur Internet
- Mettre en place des dispositifs pour contourner la sécurité
- Modifier la configuration de son poste sans autorisation
- Se livrer à des actes de piratage

L'utilisateur doit :

- Faire usage des services Internet dans le cadre exclusif des activités professionnelles de l'organisme
- Appliquer les règles de sécurité préconisées et contribuer à la sécurité générale de l'organisme
- Prendre soin du matériel mis à sa disposition
- Informer le support informatique de toute anomalie constatée

### 3.2.2 Sécurité des connections WIFI (LAN/WLAN, …)

Les réseaux Wifi ont permis une plus grande facilité d'accès au réseau. En effet, sans fils, ces réseaux présentent l'avantage certain d'une plus grande aisance d'accès, de couverture et de navigation à haut débit et de s'affranchir des câbles et connectiques classiques.

Cependant ces réseaux sont connus pour être faillibles tant au niveau de l'accès, qu'au niveau de l'intégrité et de l'authenticité des données.

Voici quelques démarches simples pour sécuriser son accès au Wifi :

- Ne faites jamais confiance aux réseaux de Wi-Fi public qui ne demandent pas de mots de passe. Les cybercriminels créent souvent ce type de réseaux pour fouiner dans les données personnelles des utilisateurs
- Désactivez le Wi-Fi si vous ne l'utilisez pas. Cette mesure protégera vos données et vous aidera à économiser la durée de vie de la batterie de votre appareil. Vérifiez si votre appareil est réglé pour se connecter automatiquement aux réseaux Wi-Fi inconnus. Si c'est le cas, désactivez cette fonction. Cette mesure vous permettra également de vous protéger des méthodes de traçage utilisées par différentes organisations.
- Les cas de stricte nécessité. Lorsque vous utilisez un réseau Wi-Fi public, n'ouvrez pas votre compte bancaire ou d'autres services importants.
- Envisagez l'utilisation d'un réseau privé virtuel ou VPN au-dessus de la connexion Wifi. C'est une bonne méthode pour protéger les données de vos collaborateurs et de votre entreprise étant donné qu'un service VPN chiffre tout ce que vous envoyez.

### 3.2.3 Sécurité du site

Un autre aspect de la sécurité web concerne le site de votre entreprise. En effet, il s'agit de la vitrine de votre activité, et est souvent attrayante pour les pirates qui souhaitent apporter une atteinte à votre image, à votre revenu, ou à votre infrastructure. Souvent le site web, mal sécurisé, constitue une porte d'entrée pour les attaques sophistiquée.

La plupart des attaques web ont pour cause les éléments suivants :

- Injection de code
- Mauvaise configuration de sécurité
- Exposition de données sensibles

Voici quelques mesures pour sécuriser votre site web :

#### Maintenir une infrastructure logicielle à jour

Et ceci en mettant à jour le serveur web qui héberge le site. Si vous sous-traitez cette activité, c'est le travail de votre hébergeur, contrôlez le et n'hésitez pas à vérifier constamment la version de votre site web et du serveur vis-à-vis de la dernière version publiée.

Le système de gestion du site (CMS …) doit être à jour. Ainsi que les additions (plugins) installés avec votre système de gestion de contenu. Les failles sont connues et répertoriées, avoir la dernière version est votre assurance pour être sécurisé contre l'ensemble des failles récentes.

#### Back up et protection

Comme pour toutes les données sensibles de l'entreprise, il est nécessaire de faire une sauvegarde régulière de votre site web. Ce backup aura une valeur inestimable si votre site web se fait attaqué malgré vos précautions.

Ensuite, l'accès aux arborescences privées de votre site doit être protégé, seules les pages du site doivent être visibles de l'extérieur.

L'authentification http est l'une des protections possibles pour votre serveur web

#### Données sensibles

Lorsque vous collectez des données sensibles (données personnelles, mots de passe, données financières…), il faut les protéger mieux que tout le reste. Il s'agit non seulement d'une obligation vis-à-vis de vos utilisateurs, mais aussi d'une contrainte légale. Consultez la CNPD pour savoir précisément quelles sont vos obligations en la matière.

La connexion doit elle aussi être chiffrée (ssl) pour éviter que des données soient interceptées lors de la communication entre l'utilisateur et votre site, mettez en place un certificat SSL sur votre site pour assurer la protection des données de vos utilisateurs.

Toutes les informations doivent être cryptées avant d'être stocké pour une meilleure protection en cas de subtilisation des données.

#### A faire et à ne pas faire

Rappelons ces simples directives pour maintenir une utilisation correcte des moyens informatiques et de télécommunications mis à disposition par l'entreprise aux collaborateurs :

### A Faire :

- Faire usage des services Internet dans le cadre exclusif des activités professionnelles
- Appliquer les règles de sécurité préconisées et contribuer à la sécurité générale de l'organisation et de l'entreprise.
- Prendre soin du matériel mis à sa disposition.
- Informer le service informatique de toute anomalie constatée.

### A ne pas faire :

- Utiliser des moyens de connexion autre que ceux offerts par votre organisme (4G, etc.)
- Télécharger de fichier depuis des sites douteux.
- Utiliser les postes de travail ou l'identité d'autres personne pour naviguer l'internet.
- Naviguer sur des sites douteux ou à caractère immoral.
- Effectuer de téléchargements illégaux.
- Divulguer sur Internet des informations à caractère confidentiel ou pouvant porter préjudice à l'organisation.
- Abuser de la navigation sur Internet (en temps et en volume).
- Mettre en place des dispositifs pour contourner la sécurité.
- Modifier la configuration de son poste sans autorisation.
- Se livrer à des actes de piratage.

## 3.3 Diverses facettes de la cybercriminalité

### 3.3.1 Vecteurs d'attaques cybercriminelles

**Malware :** Un logiciel malveillant ou maliciel (en anglais : malware) est un programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté. Les malwares englobent les virus, les vers, les chevaux de Troie, ainsi que d'autres menaces.

**Ransomware :** Logiciel malveillant qui prend en otage des données personnelles. Pour ce faire, un ransomware chiffre des données personnelles puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer. Un ransomware peut aussi bloquer l'accès de tout utilisateur à une machine jusqu'à ce qu'une clé ou un outil de débridage soit envoyé à la victime en échange d'une somme d'argent.

#### Les plus grandes cyberattaques qui ont frappé le monde en 2017

**WannaCry :** En mai 2017, il est utilisé lors d'une cyberattaque mondiale massive, touchant plus de 300 000 ordinateurs, dans plus de 150 pays et utilisant le système obsolète Windows XP.

**NotPetya :** En Juin 2017, Le virus, baptisé NotPetya, est un ransomware, à l'instar de WannaCry, qui a touché des centaines de milliers d'ordinateurs en mai. Ce qui veut dire que les données de l'utilisateur sont chiffrées et impossible à utiliser, à moins de payer une rançon pour obtenir une clé de déchiffrement.

**Facebook security breach :** On September 2017, Up to 50m accounts attacked.
« *On Tuesday, we discovered that an attacker exploited a technical vulnerability to steal access tokens that would allow them to log into about 50 million people's accounts on Facebook* »: a indiqué Mark Zuckerberg le 28/09/2018 dans un message publié sur sa propre page

**Extorsion :** L'extorsion est définie comme une « infraction consistant à obtenir la remise de fonds, d'un bien quelconque, ou une signature, un engagement, une renonciation ou la révélation d'un secret, au moyen de violences, menaces ou contrainte, l'extorsion numérique des entreprise la plus courante est celle d'une attaque par déni de service distribué (DDoS), ciblant les sites des entreprises en les parallélisant, et ensuite demander une rançon. Les entreprises ne doivent en aucun cas accepter de payer la rançon, sous peine de créer un dangereux précédent et d'encourager d'autres attaques à l'avenir.

**Virus :** Programme de très petite taille qui possède la faculté de s'introduire dans un programme hôte, et de s'auto-reproduire chaque fois que celui-ci démarre. Son but est généralement de détruire ou de falsifier des fichiers de données ou des fichiers de systèmes d'exploitation.

**Ver informatique :** un logiciel malveillant qui se reproduit sur plusieurs ordinateurs en utilisant un réseau informatique comme Internet. Il vise à rendre le réseau inaccessible par la saturation sa bande passante.

**Cheval de Troie (troyen ou trojan horse) :** Programme qui apparaît légitime alors qu'il contient un autre programme capable de générer des actions illégales. Souvent confondu avec les virus ou autres parasites, le programme lui-même n'étant pas un virus mais un véhicule innocent utilisé pour faire entrer ce parasite sur l'ordinateur et de l'y installer à l'insu de l'utilisateur pour accéder frauduleusement à des ressources.

**Keylogger :** Programme qui espionne et enregistre tout ce que l'utilisateur saisit sur son clavier.

**Spam :** E-mail non sollicité par les destinataires, contenant ou non une pièce jointe, et généralement mensongers (dit aussi « junk mail »), expédié en masse à une multitude de destinataires n'ayant sollicité aucune demande de la part de l'émetteur, à des fins publicitaires ou malhonnêtes. Utilisé pour promouvoir des services ou des produits commerciaux, il contribue à la pollution voir à la saturation des boîtes aux lettres électroniques.

**Spyware (logiciel espion) :** Logiciel parasite indétectable destiné à collecter et de transmettre à des tiers des informations sur les habitudes de navigation d'un utilisateur ou encore des informations personnelles (adresse e-mail, mots de passe, …), pour des buts « commerciaux malsains » sans avoir une action destructive.

## Mesures de protection :

- Installer un antivirus (logiciel qui protège un ordinateur contre les virus, et de plus en plus contre d'autres malwares : «trojans», scripts malicieux dans les pages web, etc.) et mettez-le régulièrement à jour, en activant l'option de mise à jour automatique de l'anti-virus ;
- Passer systématiquement à l'antivirus tout support numérique extérieur et refuser la connexion d'un équipement dont on ne connaît pas la provenance ;
- Corriger et mettre à jour le système d'exploitation : Un système sans mise à jours de sécurité est un système vulnérable, ouvert à tout type d'attaques (virus, attaques directes), il renferme des failles de sécurité (erreur de programmation), qui doivent être corrigés via l'application des « Patchs » correspondants, publiés par l'éditeur ;
- Sauvegarder régulièrement les données importantes : Sauvegarder régulièrement vos données sur des supports amovibles (disquettes, CDs, …), car un virus pourrait endommager les fichiers et les données stockées sur le disque ;
- Utiliser un logiciel antispam pour bloquer ou déplacer les emails indésirables ;
- Utiliser un logiciel antispyware ;
- Utiliser un logiciel antiKeylogger.

### 3.3.2 Piratage, Hacking, fraude, phishing, spofing

**Les pirates** désignent des spécialistes en informatiques dont les actions sont nuisibles. Selon leurs actions ils peuvent être qualifiés de hackers blacks hats, de crackers ou encore d'hacktivistes.

**Le hacking** est un ensemble de techniques informatiques, visant à attaquer un réseau, un site, etc. Ces attaques sont diverses. On y retrouve :

- L'envoi de "bombes" logicielles.
- L'envoi et la recherche de chevaux de Troie.
- La recherche de trous de sécurité.
- Le détournement d'identité.
- La surcharge provoquée d'un système d'information (Flooding de Yahoo, eBay...).
- Changement des droits utilisateur d'un ordinateur.
- La provocation d'erreurs non gérées, etc.

Les attaques peuvent être locales (sur le même ordinateur, voir sur le même réseau) ou distantes (sur internet, par télécommunication).

Il y a différentes motivations au hacking. Selon les individus (les "hackers"), on y retrouve :

- Vérification de la sécurisation d'un système.
- Vol d'informations (fiches de paye...).
- Terrorisme.
- Espionnage "classique" ou industriel.
- Chantage.
- Manifestation politique.
- Pour gagner de l'argent.
- Par simple "jeu", par défi.
- Pour apprendre, etc.

Alors que le hacker black hat est un expert en informatique qui utilise ses connaissances de façon nuisible. Il doit être différencié du hacker white hat qui est un spécialiste informatique qui n'a pas de but nuisible. Les hackers white hats sont essentiels: ils sont les moteurs de l'informatique moderne et ils contribuent à sa sécurisation.

- **Phishing (hameçonnage) :** Technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. La technique consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance - banque, administration, etc. - afin de lui soutirer des renseignements personnels : mot de passe, numéro de carte de crédit, date de naissance, etc. L'hameçonnage peut se faire par courrier électronique, par des sites web falsifiés ou autres moyens électroniques.

- **Spoofing (usurpation d'identité électronique) :** Technique qui consiste à usurper l'identité (ou voler l'identité) d'un utilisateur sur Internet (ou au sein d'un réseau en général), afin de faire croire que les actions ou communications faites proviennent de quelqu'un d'autre (l'utilisateur dont on a usurpé l'identité).

### 3.3.3 Blanchiment de fond, Monnaies virtuelles

- **Monnaies virtuelles :** Les monnaies virtuelles ont été conçues comme une alternative à la monnaie légale, initialement développées au sein de communautés virtuelles, notamment dans le cadre des jeux en ligne. Elles se sont multipliées tandis que leurs possibilités d'utilisation se sont élargies et s'étendent à la sphère réelle. De très nombreuses monnaies virtuelles sont désormais en circulation comme le Bitcoin (1Bitcoin=environ 380 euro). Les monnaies virtuelles peuvent être employées pour régler des transactions sur internet, mais également peuvent être dépensées dans l'économie réelle auprès de commerçants les acceptants.

- **Blanchiment de fond :** Grâce aux monnaies virtuelles Du fait de leurs caractéristiques (extraterritorialité et absence d'organe de régulation notamment) et de leur mode de fonctionnement, les monnaies virtuelles présentent des risques intrinsèques et sont de nature à permettre le financement d'activités criminelles et à faciliter le blanchiment du produit de celles-ci.

  L'anonymat offert par la monnaie virtuelle permet aux auteurs des infractions de se faire remettre des fonds sans laisser de trace de la transaction, elle s'apparente en cela à une transaction en espèces qui peut néanmoins être effectuée sur Internet sans que jamais auteurs et victimes ne se rencontrent. Dans ce contexte, elle s'inscrit dans une délinquance traditionnelle qui s'adapte aux évolutions technologiques et aux possibilités offertes.

### 3.3.4 Escroquerie sur les moyens de payement

Lorsque vous réalisez des achats sur Internet, via votre ordinateur ou votre ordiphone (smartphone), vos coordonnées bancaires sont susceptibles d'être interceptées par des attaquants directement sur votre ordinateur ou dans les fichiers clients du site marchand. Ainsi, avant d'effectuer un paiement en ligne, il est nécessaire de procéder à des vérifications sur le site Internet :

- Contrôlez la présence d'un cadenas dans la barre d'adresse ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs) ;
- Assurez-vous que la mention « https:// » apparait au début de l'adresse du site Internet ;
- Vérifiez l'exactitude de l'adresse du site Internet en prenant garde aux fautes d'orthographe par exemple. Si possible, lors d'un achat en ligne ;
- Privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS ;
- De manière générale, ne transmettez jamais le code confidentiel de votre carte bancaire ;
- N'hésitez pas à vous rapprocher de votre banque pour connaître et utiliser les moyens sécurisés qu'elle propose.

## 3.4 Mesures de sécurité des échanges et transactions électroniques

### 3.4.1 Menaces sur le courrier électronique

Parmi les menaces sur le courrier électronique : Infection par un malware, Vol d'identité, Divulgation d'information, phishing.

Quelques Mesures de protection :

- Ne pas ouvrir les courriers électroniques douteux ou d'expéditeurs inconnus.
- Appliquer les mécanismes anti-piratage prévus par chaque serveur de mail (gmail, yahoo, msn, live, hotmail).
- L'identité d'un expéditeur n'étant en rien garantie : vérifiez la cohérence entre l'expéditeur présumé et le contenu du message et vérifier son identité. En cas de doute, ne pas hésiter à contacter directement l'émetteur du mail ;

- N'ouvrez pas les pièces jointes provenant de destinataires inconnus ou dont le titre ou le format paraissent incohérents avec les fichiers que vous envoient habituellement vos contacts ;
- Ne répondez jamais par courriel à une demande d'informations personnelles ou confidentielles (ex : code confidentiel et numéro de votre carte bancaire)
- N'ouvrez pas et ne relayez pas de messages de types chaînes de lettre, appels à la solidarité, alertes virales, etc. ;
- Choisissez un mot de passe fort, pour votre courrier électronique ;
- Choisissez un mot de passe qui n'est pas lié à votre identité (mot de passe composé d'un nom de société, d'une date de naissance, etc.)
- Utilisez des mots de passe différents pour vous authentifier auprès de systèmes distincts en particulier, la messagerie professionnelle celle personnelle ;
- Renouvelez vos mots de passe avec une fréquence raisonnable ;
- Configurez les logiciels, y compris votre navigateur web, pour qu'ils ne se "souviennent" pas des mots de passe choisis ;
- Appliquer les options de sécurité offertes par votre fournisseur ;
- Ne jamais poster votre email dans les forums et les blogs ;
- Essayer d'avoir deux emails, un email public pour les sites qui demandent un enregistrement pour téléchargement ou autre et un deuxième privé ;
- Ne jamais répondre à un spam ;
- Ne jamais cliquer sur un lien html dans un email spam ;
- Ne jamais cliquer sur la pièce jointe d'un spam ;
- Utiliser un logiciel antispam pour bloquer ou déplacer les emails indésirables ;
- Désactivez l'ouverture automatique des documents téléchargés et lancez une analyse antivirus avant de les ouvrir afin de vérifier qu'ils ne contiennent aucune charge virale connue ;
- Ne jamais suivre un email qui demande des informations personnelles et confidentielles par courrier électronique ;
- Optimiser la configuration de son antivirus vis-à-vis de la messagerie électronique
- Bloquer images et contenus externes dans les messages HTML.

### 3.4.2 Mot de passe

Les mots de passe sont largement utilisés pour protéger l'accès aux renseignements professionnels et aux outils en ligne, mais si les employés ne sont pas prudents, d'autres personnes peuvent utiliser leurs mots de passe afin d'accéder à des dossiers et à des renseignements cruciaux.

Voici plusieurs problèmes courants relatifs à l'utilisation des mots de passe en entreprise :

- Les employés notent leurs mots de passe et les placent à des endroits où d'autres peuvent les copier ou les divulguent tout simplement à des tiers. Dans les deux cas, la perte de contrôle de ces mots de passe fait en sorte qu'il est impossible de garantir que la personne qui accède aux systèmes est autorisée à le faire;
- Les employés utilisent des mots de passe faibles, faciles à deviner, ce qui rend possible l'accès d'autres personnes à des systèmes ou à des renseignements de nature délicate;

- Ils utilisent le même mot de passe pour plusieurs systèmes ou services de sorte que si l'un d'entre eux est compromis, tous les autres sont à risque;
- Ils ne changent pas leurs mots de passe régulièrement.
- Adoptez une politique rigoureuse en matière de mots de passe décrivant les règles qui doivent s'appliquer à ceux qui sont utilisés dans votre entreprise.

**Les directives suivantes devraient en faire partie :**

- Évitez les mots communs, comme « mot de passe » ou « connexion »;
- Évitez les séquences de nombres simples, comme « 1234 »;
- Évitez les noms propres faciles à deviner, comme le prénom d'un enfant;
- Créez des mots de passe comptant au moins huit caractères (plus le nombre de caractères est élevé, plus un mot de passe est sécuritaire);
- Créez un mot de passe fort en incluant une combinaison des éléments suivants :
- Lettres majuscules;
- Lettres minuscules;
- Chiffres;
- Caractères spéciaux (exemple : !, $, # ou %).
- Expliquez à vos employés que les mots de passe forts sont importants pour la sécurité de l'entreprise.
- Encouragez-les à suivre ces conseils pour protéger leurs mots de passe :
- Garder leurs mots de passe confidentiels;
- Changer leurs mots de passe régulièrement. Votre entreprise devrait exiger ce changement tous les trois mois;
- Éviter d'utiliser le même mot de passe pour plusieurs comptes ou systèmes.
- Vous pourriez aussi envisager l'utilisation d'un gestionnaire de mots de passe (un programme qui génère et stocke des mots de passe aléatoires) qui créera des mots de passe encore plus forts à l'usage des employés.

### 3.4.3 Divulgation d'information

Il est impératif de sensibiliser et d'impliquer le personnel de tous les services de l'entreprise, et plus particulièrement lorsqu'ils ont accès à des informations sensibles. Le personnel doit avoir conscience de ce qui est confidentiel et de la valeur des informations qu'ils créent et des informations en leur possession, ainsi que des précautions à prendre dans les contacts extérieurs afin d'éviter toute divulgation accidentelle.
Il faut également souligner que la vigilance dans la protection des informations doit aussi s'exercer à l'égard des informations confidentielles reçues par l'entreprise de ses partenaires, clients et fournisseurs.

Des mesures de restriction peuvent être prévues concernant la diffusion de certaines informations en interne (en fonction du poste occupé dans l'entreprise) et/ou à destination d'interlocuteurs extérieurs. Il est possible de créer dans l'entreprise une liste des personnes habilitées à connaître de telles informations.

Il est important de ne jamais donner d'informations personnelles ou professionnelles sur des forums (adresse physique, de messagerie…), ou réseaux sociaux.

### 3.4.4 Envois, réceptions et partage sécurisés

Une étude menée par Axwa auprès de plus de 600 professionnels de l'informatique met en évidence les dangers des services cloud publics tels que DropBox, Box et Google Docs. L'enquête « Achieving Security in Workplace File Sharing » (« Garantir la sécurité du partage de fichiers en entreprise ») révèle que près de 50 % des entreprises trouvent que les services grand public de partage de fichiers dans le cloud comme DropBox ou Google Docs ne sont pas adaptés à un usage professionnel. Les entreprises doivent conscients des conséquences catastrophiques que pourraient avoir d'éventuelles failles de sécurité de ces outils.

Un nombre croissant d'employés a recours à des solutions de partage de fichiers en ligne à usage personnel qui ne sont pas approuvées par la direction informatique de leur entreprise.

Pour sécuriser le partage de fichiers il est recommandé de :

- Centraliser le stockage et la gestion des fichiers avec un système Web sécurisé, accessible en tout lieu et avec n'importe quel appareil, pour la protection hors site des données.
- Mettre en place des contrôles et des autorisations d'accès pour sécuriser les fichiers privés et les séparer des fichiers de production.
- Surveiller les modalités de partage des fichiers de l'entreprise.
- Mettre en place un système évolutif qui accompagne la croissance de l'entreprise.

## 3.5 La sécurité des données

### 3.5.1 Stockage, sauvegarde et restauration des données

Pour veiller à la sécurité de vos données, il est vivement conseillé d'effectuer des sauvegardes régulières (quotidiennes ou hebdomadaires par exemple). Vous pourrez alors en disposer suite à un dysfonctionnement de votre système d'exploitation ou à une attaque.

Pour sauvegarder vos données, vous pouvez utiliser des supports externes tels qu'un disque dur externe réservé exclusivement à cet usage, ou, à défaut, un CD ou un DVD enregistrable que vous rangerez ensuite dans un lieu éloigné de votre ordinateur, de préférence à l'extérieur de l'entreprise pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde en cas d'incendie ou d'inondation ou que la copie de sauvegarde ne soit volée en même temps que l'ordinateur contenant les données d'origine. Néanmoins, il est nécessaire d'accorder une attention particulière à la durée de vie de ces supports.

### 3.5.2 Transfert des données et Cloud computing/ virtualisation

Avant d'effectuer des sauvegardes sur des plateformes sur Internet (souvent appelées « cloud » ou « informatique en nuage »), soyez conscient que ces sites de stockage peuvent être la cible d'attaques informatiques et que ces solutions impliquent des risques spécifiques :

- Risques pour la confidentialité des données,
- Risques juridiques liés à l'incertitude sur la localisation des données,
- Risques pour la disponibilité et l'intégrité des données,
- Risques liés à l'irréversibilité des contrats.

soyez vigilant en prenant connaissance des conditions générales d'utilisation de ces services. Les contrats proposés dans le cadre des offres génériques ne couvrent généralement pas ces risques ;

autant que possible, n'hésitez pas à recourir à des spécialistes techniques et juridiques pour la rédaction des contrats personnalisés et appropriés aux enjeux de votre entreprise ;

veillez à la confidentialité des données en rendant leur lecture impossible à des personnes non autorisées en les chiffrant à l'aide d'un logiciel de chiffrement avant de les copier dans le « cloud ».

### 3.5.3 Sécurité des données de la PME vs la Mobilité

L'emploi d'ordinateurs portables, d'ordiphones (smartphones) ou de tablettes facilite les déplacements professionnels ainsi que le transport et l'échange de données.

Voyager avec ces appareils nomades fait cependant peser des menaces sur des informations sensibles dont le vol ou la perte auraient des conséquences importantes sur les activités de l'organisation.

#### Avant de partir en mission :

N'utilisez que du matériel (ordinateur, supports amovibles, téléphone) dédié à la mission, et ne contenant que les données nécessaires ;

Sauvegardez ces données, pour les retrouver en cas de perte ;

Si vous comptez profiter des trajets pour travailler, emportez un filtre de protection écran pour votre ordinateur ; apposez un signe distinctif (comme une pastille de couleur) sur vos appareils pour vous assurer qu'il n'y a pas eu d'échange pendant le transport

#### Pendant la mission :

Gardez vos appareils, supports et fichiers avec vous, pendant votre voyage comme pendant votre séjour (ne les laissez pas dans un bureau ou un coffre d'hôtel) ;

Désactivez les fonctions Wi-Fi et Bluetooth de vos appareils ;

Retirez la carte SIM et la batterie si vous êtes contraint de vous séparer de votre téléphone ;

### 3.5.4 Collecte et tri des données personnelles

La collecte et le tri des données personnelles doit respecter les dispositifs de la loi 09-08 relative au traitement des données personnelles. Pour collecter les données personnelles, les entreprises doivent respecter six règles d'or suivantes :

- Veiller à la sécurité des fichiers ;
- Assurer la confidentialité des données ;
- Informer les personnes concernées de leurs droits ;
- Demander l'autorisation à la CNDP;
- Fixer une date de conservation raisonnable des données périssables ;
- Définir un objectif précis au traitement des données.

## Evaluation

## Maturité

# 4. QUESTIONNAIRE SUR LA MATURITE DE LA SECURITE DES SI

La norme ISO/IEC 21827 définit 5 niveaux de maturité SSI. Ils représentent la manière dont une organisation exécute, contrôle, maintient et assure un suivi d'un processus :

Cependant, adopter une démarche globale d'excellence opérationnelle et de création de valeur prend du temps, et nécessite de franchir progressivement les 5 niveaux de maturité :

- Niveau 1 - Pratique informelle
- Niveau 2 - Pratique répétable et suivie : des actions reproductibles
- Niveau 3 - Processus défini : la standardisation de pratiques
- Niveau 4 - Processus contrôlé : la mesure quantitative
- Niveau 5 - Processus optimisé : l'amélioration continue

Le questionnaire suivant peut servir comme base permettant de simuler son niveau de maturité SSI.

### Question n°1 : Comment qualifieriez-vous votre système d'information ?

0- Le système d'information est un outil facilitant le travail sans intervenir directement dans les directions métiers

1- Le système d'information est le moyen d'avoir une vision transverse des processus et de l'organisation de l'organisme, il constitue une aide à la décision

2- Le système d'information est un outil de transformation organisationnelle et d'amélioration de la performance opérationnelle

3- Le système d'information est un outil indispensable au fonctionnement de l'organisation, mais sa contribution est difficile à mesurer, bien que les dépenses informatiques doivent être maîtrisées

### Question n° 2 : Quel est l'effet de la perte du SI (Indisponibilité) sur le fonctionnement ?

0- Aucun effet

1- Un effet faible, l'activité est faiblement déstabilisée puis s'autorégule

2- Un effet majeur, l'activité est fortement entravée dans l'attente d'un retour à la normale

3- Un effet bloquant, provoque l'arrêt de l'activité dans l'attente d'un retour à la normale

### Question n° 3 : Quel est l'effet d'une perte d'intégrité de l'information sur le fonctionnement ?

0- La perte d'intégrité n'a pas d'effet sur le fonctionnement

1- La perte d'intégrité à un effet faible, elle n'engendre que peu de dysfonctionnement

2- La perte d'intégrité a un effet majeur, les dysfonctionnements sont importants et remettent en cause temporairement la poursuite de l'activité

3- La perte d'intégrité a un effet bloquant, des dysfonctionnements majeurs (arrêt d'activité, perte d'image, perte de clients, etc.) sont à craindre

### Question n° 4 : Quel est l'effet de la divulgation d'informations sur le fonctionnement ?

0- La divulgation d'informations n'a aucun effet sur le fonctionnement

1- La divulgation d'information a un effet faible, la pérennité de l'activité en serait peu menacée, pas de risque juridique

2- La divulgation d'information a un effet majeur, entraînant la perte d'un avantage concurrentiel important, une perte de crédibilité importante ou un risque juridique important

3- La divulgation d'information a un effet bloquant, la survie de l'activité est remise en cause ou un risque majeur existe

### Question n° 5 : Comment décririez-vous l'environnement concurrentiel de votre entreprise ?

0- Pas concurrentiel ou pas menace d'agence gouvernementale (administration)

1- Peu concurrentiel ou menace d'agence faible

2- Concurrentiel ou menace d'agence classique

3- Concurrence féroce ou menace d'agence majeure

### Question n° 6 : Le secteur d'activité est-il innovant ?

0- Secteur non innovant / pas d'avance technologique

1- Secteur à faible innovation / avance technologique peu significative

2- Secteur à forte innovation / avance technologique importante

3- Secteur de type R&D exclusivement / avance technologique déterminante

### Question n° 7 : Quel est le niveau d'interconnexion du SI ?

0- Système isolé

1- Système intranet ou connexions restreintes avec partenaires identifiés

2- Système extranet fortement interconnecté

3- Système et ou services sur Internet

### Question n°8 : Quel est le niveau d'homogénéité du SI ?

0- Système très standardisé

1- Système peu hétérogène

2- Système hétérogène

3- Système fortement hétérogène

### Question n°9 : Sous-traitance d'exploitation et/ou exploitation interne du SI ?

0- Autonomie, pas d'appel à sous-traitance

1- Utilisation limitée de la sous-traitance et/ou mise en place de contrats et de procédures rigoureuses concernant les exploitants

2- Utilisation relativement importante de la sous-traitance et/ou mise en œuvre de clauses contractuelles spécifiques de "qualité" du personnel exploitant

3- Utilisation importante de la sous-traitance et/ou aucune règle mise en place concernant le personnel exploitant

### Question n°10 : Politique de Sécurité

0- Aucune politique de sécurité, l'entreprise n'est pas sensibilisée à la sécurité

1- Un usage occasionnel et informel de bonnes pratiques fait office de référentiel SSI

2- Un référentiel des meilleures pratiques existe et permet la gestion de la SSI, (planification, vérification, actions correctives)

3- La politique de sécurité est formalisée à l'aide d'outils méthodologiques définis

4- Des objectifs mesurables sont définis, une organisation prévoit le suivi de ces objectifs

5- La politique de sécurité est inscrite dans un processus d'amélioration continu

### Question n° 11 : Organisation de la sécurité

0- Organisation inexistante

1- Organisation SSI informelle

2- La SSI est gérée (planification, vérification, actions correctives)

3- Responsabilités et procédures SSI formalisées et généralisées

4- Définition d'objectifs mesurables et suivi de la mise en œuvre de l'organisation SSI

5- Amélioration continue de l'organisation SSI

### Question n° 12 : Gestion des risques SSI

0- Aucune gestion des risques SSI

1- Usage occasionnel de meilleures pratiques pour gérer les risques SSI

2- Gestion des meilleures pratiques pour gérer les risques SSI (planification, vérification, actions correctives)

3- Usage généralisé d'outils méthodologiques pour gérer les risques SSI

4- Définition d'objectifs mesurables et suivi de la gestion des risques SSI (indicateurs, tableaux de bord ssi, audits...)

### Question n° 13 : Gestion les actifs

0- Aucune gestion des actifs

1- Usage occasionnel de meilleures pratiques pour gérer les actifs

2- Gestion des meilleures pratiques pour gérer les actifs (Responsabilité, classification, etc...)

3- Usage généralisé d'outils méthodologiques pour gérer les actifs

4- Définition d'objectifs mesurables est suivi de la gestion des actifs (indicateurs, tableaux de bord, audit...)

5- Réitération régulière des processus de gestion des risques SSI

### Question n° 14 : Documentation

0- Aucune documentation de la SSI

1- Rédaction occasionnelle de documentation SSI (ex : conception, recette, exploitation,...),

2- Gestion d'une documentation SSI homogène (Planification, vérification, actions correctives)

3- Formalisation d'un cadre de gestion documentaire de la SSI

4- Comparaison régulière de la documentation SSI avec la réalité

5- La documentation SSI est mise à jour régulièrement et comporte un volet d'enregistrement des événements et du reporting conforme ISO 27001

### Question n° 15 : Sécurité des ressources humaines

0- Les aspects humains ne sont pas pris en compte dans la SSI

1- Prise en compte occasionnelle des aspects humains dans la SSI (ex : recrutements, habilitations,...)

2- Intégration systématique des aspects humains dans la SSI,

3- Un processus défini des gestions des aspects humains est mis en œuvre, les procédures RH tiennent compte de la SSI (Embauches, Modifications, fin de contrat,...)

4- Définition d'objectifs mesurables et suivi du personnel

5- Optimisation continue des processus SSI liés aux ressources humaines

## Question n°16 : Sensibilisation et formation

0- Aucune sensibilisation ni formation en matière de SSI

1- Sensibilisations et formations occasionnelles (auto-formations...)

2- Sensibilisations et formations gérées formellement

3- Formalisation d'un plan de formation défini, adapté aux profils des personnels ou éventuellement usage de "certification" des individus

4- Définition d'objectifs mesurables et évaluation des personnels suite aux sessions de sensibilisation et de formations

5- Amélioration continue du plan de formation en fonction des retours d'expériences

## Question n° 17 : Sécurité physique et environnementale

0- Aucunes règles de protection d'accès physiques aux locaux ou à des zones sécurisées spécifique à la SSI

1- Mise en œuvre de mesures relatives aux aspects de sécurité physique ou environnementaux sur la base de l'expertise individuelle

2- Mise en œuvre de mesures relatives aux aspects de sécurité physique ou environnementaux sur la base de meilleures pratiques partagées

3- Exploitation des résultats d'une analyse des risques SSI pour la définition et la mise en œuvre des mesures de sécurité relatives aux aspects physiques et environnementaux

4- Définition d'objectifs mesurables et suivi de la mise en œuvre des mesures de sécurité relatives aux aspects physiques et environnementaux

5- Amélioration continue des procédures de mise en œuvre des mesures de sécurité relatives aux aspects physiques et environnementaux

## Question n° 18 : Exploitation et Réseaux

0- Aucune procédure ou règle d'exploitation ou réseau spécifique à la SSI

1- Mise en œuvre des règles et procédures d'exploitation ou réseau relatives à la ssi sur de l'expertise individuelle

2- Mise en œuvre des règles et procédures d'exploitation ou réseau relatives à la SSI sur de meilleures pratiques partagées (gestion des modifications, séparation des tâches avec les etudes, sauvegardes, sécurité des réseaux, ...)

3- Exploitation des résultats d'une analyse des risques pour la définition et la mise en œuvre des règles et procédures d'exploitation ou réseau relatives à la SSI

4- Définition d'objectifs mesurables et suivi de la mise en œuvre des règles et procédures d'exploitation ou réseau relatives à la SSI

5- Amélioration continue des procédures et règles d'exploitation ou réseau

## Question n° 19 : Contrôles d'accès logique, Identification / Authentification

0- Pas de règle ni de procédure pour la mise en œuvre des mécanismes de contrôle d'accès et d'identification / authentification

1- Définition de règles et procédures pour la mise en oeuvre de mécanismes de contrôle d'accès logique et d'identification / authentification sur la base de l'expertise individuelle

2- Définition de règles et procédures pour la mise en oeuvre de mécanismes de contrôle d'accès logique et d'identification / authentification sur la base de meilleures pratiques partagées

3- Exploitation des résultats d'une analyse des risques SSI pour la définition des mécanismes de contrôle d'accès logique, d'identification / authentification et règles ou procédures associées

4- Définition d'objectifs mesurables et suivi des mécanismes de contrôle d'accès logique, d'identification / authentification et règles ou procédures associées

5- Amélioration continue des mécanismes de contrôle d'accès logique, identification / authentification et règles ou procédures associées

### Question n° 20 : Acquisition, développement et maintenance des SI

0- Aucune prise en compte de la SSI dans les projets

1- Usage occasionnel de meilleures pratiques dans le cadre des projets

2- Gestion de meilleures pratiques dans le cadre des projets (planification, vérification, actions correctives)

3- Définition d'un dossier de sécurité et de l'intégration de la SSI dans les projets (ex : utilisation d'une méthode…)

4- Définition d'objectifs mesurables et suivi de l'intégration de la SSI dans les projets (ex : tableaux de bord projets intégrant la SSI, audits…)

5- Amélioration continue de l'intégration de la SSI dans les projets

### Question n° 21 : Cryptographie et infrastructure de gestion de clés cryptographiques (IGC)

0- Aucune IGC

1- Mise en place de fonctionnalités de gestion de clés cryptographiques sans procédure formalisée

2- Mise en place de fonctionnalités de gestion de clés cryptographiques de manière cohérente et mutualisée (planification, vérification, actions correctives)

3- Définition d'un dossier de sécurité des IGC (ex : politique de certification, déclaration des procédures de certification…)

4- Définition d'objectifs mesurables et suivi de la mise en œuvre des IGC

5- Amélioration continue des IGC (politique, procédures et mise en œuvre)

### Question n° 22 : Gestion des incidents liés à la sécurité des systèmes d'information

0- Incidents SSI non traités

1- Remontée occasionnelle et informelle d'incidents SSI

2- Incidents gérés systématiquement, mais de manière non formalisée (planification, vérification, actions correctives)

3- Gestion des incidents formalisée (ex : changements d'états, réseau de détection et d'alerte, procédure d'escalade, procédure de traitement…), exploitation des données des CSIRTs (Computer Security Incident Response Teams)

4- Définition d'objectifs mesurables et suivi de la gestion des incidents (ex : helpdesk…)

5- Gestion des incidents en constante amélioration, alimentation de bases de données d'incidents et de traitements d'incidents et interaction

### Question n° 23 : Plan de continuité d'activité

0- Aucun plan pour assurer la continuité des opérations

1- Mise en œuvre occasionnelle et de manière non formalisée de mesures de sécurité relatives à la disponibilité du système d'information (ex : sauvegardes, redondance, transfert de compétences…)

2- Gestion de meilleures pratiques relatives à la planification de la continuité (planification, tests, actions correctives)

3- Planification de la continuité formalisée (changements d'états, récupération des données, des applications, des machines, des personnels)

4- Définition d'objectifs mesurables relatifs à la planification de la continuité

5- Amélioration continue de la planification de la continuité

### Question n°24 : Conformité légale & réglementaire

0- Aucune mesure formalisée concernant le respect des lois et règlements relatifs aux TIC

1- Définition de règles et procédures pour le respect des lois et règlements relatifs aux TIC sur la base de l'expertise individuelle

2- Mise en œuvre de mesures relatives au respect des lois et règlements relatifs aux TIC sur la base des meilleures pratiques partagées

3- Exploitation des résultats d'une analyse des risques SSI pour la définition et la mise en œuvre des mesures de sécurité relatives au respect des lois et règlements relatifs aux TIC

4- Définition d'objectifs mesurables et suivi de la mise en œuvre des mesures de sécurité

5- Amélioration continue des procédures de mise en œuvre des mesures de sécurité relatives au respect des lois et règlements relatifs aux TIC.

### Vous avez terminé le questionnaire d'auto-évaluation :

Si le résultat est entre 0 et 20, la maturité SSI de l'entreprise est au Niveau 1.

Si le résultat est entre 20 et 40, la maturité SSI de l'entreprise est au Niveau 2.

Si le résultat est entre 40 et 60, la maturité SSI de l'entreprise est au Niveau 3.

Si le résultat est entre 60 et 80, la maturité SSI de l'entreprise est au Niveau 4.

Si le résultat est entre 80 et 102, la maturité SSI de l'entreprise est au Niveau 5.

Niveau 1 - Pratique informelle

Niveau 2 - Pratique répétable et suivie : des actions reproductibles

Niveau 3 - Processus défini : la standardisation de pratiques

Niveau 4 - Processus contrôlé : la mesure quantitative

Niveau 5 - Processus optimisé : l'amélioration continue

# 5. ANNEXES

## 5.1 Les 12 bonnes pratiques de base de Cybersécurité

Choisir avec soin ses mots de passe

Mettre à jour régulièrement vos logiciels

Bien connaître ses utilisateurs et ses prestataires

Effectuer des sauvegardes régulières

Sécuriser l'accès Wi-Fi de votre entreprise

Être prudent avec son ordiphone (smartphone) ou sa tablette qu'avec son ordinateur

Protéger ses données lors de ses déplacements

Être prudent lors de l'utilisation de sa messagerie

Télécharger ses programmes sur les sites officiels des éditeurs

Être vigilant lors d'un paiement sur Internet

Séparer les usages personnels des usages professionnels

Prendre soin de ses informations personnelles, professionnelles et de son identité numérique

## 5.2 Les bonnes reflexes en cas d'incident

En cas d'attaque, d'incident ou de comportement inhabituel (impossibilité de se connecter, activité importante, connexions ou activités inhabituelles, services ouverts non autorisés, fichiers créés, modifiés ou supprimés sans autorisation sur votre poste, il faut avoir les bonnes réflexes et surtout ne pas paniquer ;

Déconnectez la machine du réseau, pour stopper l'attaque. En revanche, maintenez là sous tension et ne la redémarrez pas, pour ne pas perdre d'informations utiles pour l'analyse de l'attaque

Prévenez votre hiérarchie, ainsi que le responsable de la sécurité, au téléphone ou de vive voix, car l'intrus peut être capable de lire les courriels. Prenez également contact avec un prestataire informatique qui vous aidera dans la restauration de votre système ainsi que dans l'analyse de l'attaque ;

Faites une copie physique du disque ;

Faites rechercher les traces disponibles liées à la compromission. Un équipement n'étant jamais isolé dans un système d'information, des traces de sa compromission doivent exister dans d'autres équipements sur le réseau (pare-feu, routeurs, outils de détection d'intrusion, etc.) ;

Déposez une plainte auprès de la brigade de gendarmerie ou du service de police judiciaire compétent pour le siège de la société. Dans le cas de données personnelles, contactez la CNDP.

Après l'incident : réinstallez complètement le système d'exploitation à partir d'une version saine, supprimez tous les services inutiles, restaurez les données d'après une copie de sauvegarde non compromise, et changez tous les mots de passe du système d'information.

## 5.3 Glossaire/Définitions

**Antivirus :** logiciel informatique destiné à identifier, neutraliser et effacer des logiciels malveillants.

**Cheval de Troie :** programme qui s'installe de façon frauduleuse pour remplir une tâche hostile à l'insu de l'utilisateur (espionnage, envoi massif de spams, …).

**Confidentialité :** L'information ne doit pas être divulguée qu'à la personne, entité ou processus non autorisé.

**Cyber :** Qui se rapporte aux ordinateurs, aux logiciels, aux systèmes de communications et aux services utilisés pour accéder à Internet et y interagir.

**Cyberespace :** Ensemble de données numérisées constituant un univers d'information et

**Cyber sécurité :** Situation recherchée pour un système d'information lui permettant de résister à des événements issus du cyberespace susceptible de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises.

**Cybercriminalité :** Actes contrevenants aux traités internationaux ou aux lois nationales, utilisant les réseaux ou les systèmes d'information comme moyens de réalisation d'un délit ou d'un crime, ou les ayant pour cible.

**Cyberdéfense :** Ensemble des mesures techniques et non techniques permettant à un État de défendre dans le cyberespace les systèmes d'information jugés essentiels.

**Disponibilité :** L'information doit être rendue accessible et utilisable sur demande par une entité autorisée.

**HTTPS :** Hypertext Transfer Protocol Secure.

**Intégrité :** Le caractère correct et complet des actifs doit être préservé. L'information ne peut être modifiée que par ceux qui en ont le droit.

**Parefeu (firewall) :** Genre de barrière de sécurité placée entre divers environnements réseau. Il peut s'agir d'un dispositif spécialisé ou d'un ensemble de plusieurs composantes et techniques. Seule une transmission autorisée, telle qu'elle est définie par la politique de sécurité locale, peut avoir droit de passage.

**Phishing (hameçonnage) :** méthode d'attaque qui consiste à imiter les couleurs d'une institution ou d'une société (banque, services des impôts) pour inciter le destinataire à fournir des informations personnelles.

**PME :** Petites et moyennes entreprises.

**Poste de travail :** désigne un ordinateur de bureau fixe ou un terminal portable.

**Ressource informatiques :** ce terme désigne l'ensemble des moyens informatiques, matériels ou logiciels mis à la disposition des employés de la PME à des fins professionnelles qui requièrent un accès au système d'information.

**Sauvegarde :** Processus consistant à copier des fichiers dans un outil de stockage secondaire afin que ces copies soient disponibles en cas de besoin pour une restauration future (p. ex. après une panne d'ordinateur).

**Serveur :** Ordinateur installé dans un réseau, destiné à fournir des ressources à d'autres systèmes informatiques rattachés au réseau (il stocke et « sert » des données et des applications).

**SPAM :** courriel électronique non sollicité, à caractère souvent commercial, …

**Système d'exploitation :** logiciel qui, dans un appareil électronique, pilote les dispositifs matériels et reçoit des instructions de l'utilisateur ou d'autres logiciels.

**Système d'Information :** l'ensemble des composantes informatiques permettant la création, le stockage, ou la diffusion de l'information.

**Traçabilité :** tous les éléments liés à l'audibilité et à la preuve des transactions.

**Utilisateur :** toute personne, interne ou externe à l'organisme, qui utilise, et est habilité et autorisée à utiliser le Système d'Information dudit organisme.

**URL :** Uniform Resource Locator (localisateur uniforme de ressources).

**Virus :** programme informatique écrits et conçu par des programmeurs malintentionnés. Le virus est capable d'entrainer des dommages importants.

**WiFi :** Réseau local (RL) qui emploie des signaux radio pour transmettre et recevoir des données à des distances de quelques centaines de mètres.

## WEBOGRAPHIE

http://www.vbo-feb.be/en/business-issues/safety-and-well-being-at-work/securite-des-entreprises/la-cybercriminalite--un-defi-de-taille-pour-les-entreprises-en-2015_2015-01-21/

http://bfmbusiness.bfmtv.com/01-business-forum/la-cybersecurite-n-est-pas-qu-un-enjeu-de-protection-c-est-aussi-un-enjeu-de-business-978637.html

https://fr.wikipedia.org/wiki/Rex_Mundi

http://www.lenetexpert.fr/les-statistiques-du-numerique-usages-risques-cybercriminalite/

https://www.itu.int/net/itunews/issues/2010/09/20-fr.aspx

https://sites.google.com/site/barometredegestionstrategique/Accueil/articles/risques

http://circulaire.legifrance.gouv.fr/pdf/2009/05/cir_25550.pdf

http://ca-fr.norton.com/cybercrime-stories-sandra/article

https://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20120626_01

http://www.solutions-numeriques.com/les-outils-de-partage-de-fichiers-un-risque-majeur-de-securite/

http://eduscol.education.fr/ecogest/si/SSI/risk_conf

http://www.ssi.gouv.fr/entreprise/guide/guide-des-bonnes-pratiques-de-linformatique/

https://www.epi.asso.fr/revue/97/b97p181.htm


facebook.com/CMRPI twitter.com/CmrpiMaroc


facebook.com/AusimMaroc twitter.com/AusimMaroc

linkedin.com/in/ausim

Dépôt légal:
Bibliothèque Nationale du Royaume du Maroc,
N° Dépôt : 2017MO3962

9 789954 996720