SOMMAIRE :

Liste des Figures

LISTE DES TABLEAUX :

GLOSSAIRE :

ADRG	Advanced Database Research Group
BIA	Business Impact Analysis
CDP	Commission des Données Personnelles
CMMI	Capability Maturity Model Intégration
CRM	Customer Relationship Management
CSP	centres de services partagés
DAM	Gestion des Ressources Digitales
DSI	Directeur du Système d'Information
EBIOS	Expression of Needs and Identification of Security Objectives
ERP	Enterprise Resource Planning
IBM	International Business Machines Corporation
MEHARI	Method for Harmonized Analysis of Risk
MRP	Management des Ressources de Production
PCA	Plan de Continuité d'Activité
PCOM	Plan de Communication
PGC	Plan de Gestion de Crise
PGI	progiciel de gestion intégré
PLM	Product Lifecycle Management
PME	Petite et Moyenne Entreprise
PRA	Plan de Reprise d'Activité
PRM	Plan de Reprise Métier
PSSI	politique de sécurité des systèmes d'information
RSSI	Responsable de la Sécurité du Système d'Information

RTO	Recovery Point Objective
Saas	Software as a Service
SI	Système d'Information
SMCA	Système de management de la continuité d'activité
SMSI	système de management de la sécurité des Systèmes d'Information
SSI	sécurité des systèmes d'information
TDSI	Transmission de Données et Sécurité de l'Information
TIC	Technologies de l'Information et de la Communication

AVANT-PROPOS

Le Laboratoire d'Algèbre, de Cryptographie, de Géométrie Algébrique et Application du département de Mathématiques et Informatique de la Faculté des Sciences et Techniques de l'Université Cheikh Anta DIOP de Dakar a mis en place, sous la direction du professeur Mamadou SANGHARE en 2004, un Master de Transmission des données et Sécurité de l'Information (MTDSI) et un Master d'Algèbre Géométrie et Application avec comme Spécialité Cryptologie Tatouage Réseau Génie logiciel et base de données(MAGA).

Les masters TDSI et MAGA présentent deux filières : une filière recherche et une filière professionnelle. En TDSI, il est possible depuis l'année académique 2012-2013 de le commencer en Licence première année. Il a pour vocation essentielle de former des spécialistes en sécurité des systèmes d'information.

Les diplômés de ces masters sont des informaticiens de très haut niveau capables de proposer des solutions de sécurité sur n'importe quel support, de développer des produits de sécurité adéquats et d'auditer n'importe quel système de sécurité.

Vu sa préoccupation principale et son domaine d'action qu'est la sécurité des systèmes d'information indispensable à la survie de toute entreprise, le MTDSI et MAGA sont des formations qui allient les bases théoriques de l'enseignement supérieur aux pratiques des techniques de l'entreprise où l'expertise professionnelle est de mise.

Ces Masters offrent beaucoup de débouchés aux étudiants dont les principaux peuvent être le Développement de logiciel cryptographique, l'audit et management de la sécurité des systèmes d'information, l'étude et la mise en place de réseaux sécurisés, un responsable de sécurité informatique (RSSI) dans les établissements privés ou publics, des chiffreurs, des administrateurs de bases de données, etc...

La formation MTDSI est assurée en deux années et au terme de cette formation, l'étudiant est tenu de travailler sur un projet de mémoire qu'il devra présenter devant les membres d'un jury.

Introduction

Les Technologies de l'Information et de la Communication (TIC) sont devenues omniprésentes et représentent aujourd'hui le premier levier de modernisation et de compétitivité des économies. Elles se sont progressivement généralisées dans les entreprises depuis la fin des années 90. Les dernières années ont ainsi été marquées par une formidable accélération de l'informatisation des entreprises et l'expansion ininterrompue a débuté par la numérisation des fonctions support, puis des processus métier. Cela s'est poursuivi avec le développement des systèmes d'information.

Aujourd'hui, depuis l'arrivée de l'internet, on assiste à une explosion technologique car l'usage du numérique entraine un développement de l'autonomie au travail et un sentiment de satisfaction.

Cependant, l'utilisation explosive du numérique fait que les outils, services et réseaux informatiques constituent le quotidien de bon nombre d'employés et leurs utilisations ont provoqué beaucoup de menaces dans les entreprises surtout sur l'intégrité et la confidentialité des données. L'usage du numérique en entreprise impose à toutes les organisations d'assurer la sécurité du système d'information et la protection des données personnelles et de la vie privée. Ainsi, les questions suivantes s'imposent :

- Comment mettre en place une politique de sécurité ?
- Comment garantir l'intégrité et la confidentialité des données ?
- Comment assurer la protection des données à caractère personnel ?

Pour mener à bien ce travail, nous allons d'abord parler du cadre théorique, parler de l'importance des données en entreprise, ensuite nous allons parler des ressources numériques et de la politique de sécurité et enfin nous terminerons par l'élaboration de la politique de réglementation de l'usage du numérique en entreprise.

1ère Partie : Cadre général

Chapitre 1 : Cadre théorique

1.1 Problématique

L'évolution importante des technologies d'aujourd'hui fait que les réseaux informatiques et Internet constituent un moyen commode de communication et d'échange d'informations. Ce qui provoque des menaces de plus en plus sérieuses sur la disponibilité, la confidentialité et l'intégrité des données. Ainsi, la sécurité est devenue un problème de plus en plus préoccupant dans l'environnement de travail. Actuellement, les données sont au cœur de l'activité des entreprises et constituent un actif incorporel essentiel et un patrimoine considérable.

La digitalisation des processus, la virtualisation des stockages, la multiplication des réseaux et la banalisation des nouvelles technologies accroissent les échanges et communications de données mais aussi les exposent à des dangers toujours plus nombreux. Avec le piratage informatique, la traçabilité, le marketing-comportemental, le spam, le développement de la biométrie, la vidéosurveillance et autres technologies avancées, la protection des données devient une obligation dans une organisation quels que soient sa taille et son volume.

1.2 Les Objectifs

La mise en place d'une politique de réglementation de l'usage du numérique est très complexe, car elle implique de nombreuses tâches et de nombreux acteurs. Cela demande également une analyse fine du système d'information de l'entreprise, et des compétences à la fois techniques**,** en gestion de projet, en documentation et en communication.

Elle permet de définir un ensemble de règles pour assurer :

- La transmission des données ;
- La sécurité de l'information ;
- La vie privée des utilisateurs et des clients de l'entreprise ;
- Le contrôle des accès aux informations de l'entreprise ;
- Le cycle de vie des données.

1.3 Pertinence du sujet

Si les technologies de l'Information et de la communication sont aujourd'hui un facteur de progrès et de croissance incontestable pour les entreprises, elles sont aussi leur talon d'Achille. Une dépendance trop forte et une complexité non maîtrisée, sont synonymes de faiblesse potentielle, si elles ne sont pas bien gérées.

De ce fait, la mise en place de d'une politique de règlementation de l'usage du numérique est nécessaire pour assurer la protection des données et de la vie privée.

Il est vrai que plus les technologies évoluent, plus elles offrent une plus grande mobilité aux utilisateurs et révolutionnent les habitudes et les façons de travailler.

Cependant elles sont empreintes de risques de plus en plus forts. Il faudrait donc trouver des solutions de sécurité de l'information pour mieux préserver la sécurité des systèmes d'information et aussi les intérêts de l'entreprise.

De ce fait, la mise en place de d'une politique de règlementation de l'usage du numérique est nécessaire pour assurer la protection des données et de la vie privée.

Chapitre 2 : L'importance des données

Au quotidien, les entreprises sont amenées à collecter de nombreuses informations à caractère personnel par le biais de solutions informatiques facilitant de plus en plus la gestion des données. C'est le cas, par exemple, du traitement de données de l'entreprise par le service des ressources humaines dans le cadre des recrutements, de la gestion des carrières et des compétences, les données des clients de l'entreprise, etc. En parallèle, certaines entreprises mettent également en place des dispositifs de contrôle comme la vidéosurveillance, la cybersurveillance, la géolocalisation, etc. Dans la mesure où toute divulgation ou mauvaise utilisation des données est susceptible de porter atteinte aux droits et libertés des personnes, ou à leur vie privée. Il est donc essentiel de veiller au respect des règles de protection des données à caractère personnel. A ce titre, la loi n° 2008-12 du 25 janvier 2008 relative à la réglementation générale de la protection des données à caractère personnel, fixe un cadre à la collecte et au traitement des données personnelles. Elle met en avant cinq (5) principes à respecter en cas de collecte, de traitement et de conservation des données à caractère privé :

- La finalité du traitement,
- La proportionnalité et la pertinence des données collectées,
- La durée de conservation des données,
- La sécurité et la confidentialité des données,
- Le respect des droits des personnes.

La gestion des données personnelles est désormais au cœur du quotidien de l'entreprise. Et cela ne vaut pas seulement pour les groupes spécialisés dans les technologies de la communication, loin de là. Avec l'essor du numérique, toutes les entreprises, de la Petite et Moyenne Entreprise (PME) à la multinationale, sont conduites à traiter de plus en plus de données à caractère personnel dans le cadre de leurs activités quotidiennes. La gestion du recrutement et du fichier client, de l'annuaire du personnel, utilisation de badges, vidéosurveillance ou encore géolocalisation : toutes ces pratiques impliquent le maniement de données personnelles. Pour les entreprises, l'enjeu relatif à ces usages croissants de données n'est pas seulement de nature juridique. Il influence aussi la qualité de la relation avec leurs clients, les échanges avec leurs écosystèmes d'innovation et l'éthique interne des employés. En un mot, l'entreprise est-elle digne de confiance vis-à-vis de l'ensemble des parties prenantes qui travaillent avec elle ?

C'est particulièrement vrai depuis quelques années, alors que les individus sont de plus en plus sensibles aux risques liés à la gestion de leurs données. Dans ce contexte, la conformité peut aussi devenir un argument concurrentiel pour l'entreprise soucieuse d'attirer et de retenir les

consommateurs et partenaires. La Commission des Données Personnelles (CDP) s'est particulièrement attachée ces dernières années à accompagner les entreprises dans cette direction. Elle l'a fait en répondant à des plaintes toujours plus nombreuses et en mettant en place des stratégies pour le respect de la réglementation générale sur les données personnelles. Ces réglementations permettent de lutter contre les atteintes à la vie privée susceptibles d'être engendrées par la collecte, le traitement, la transmission, le stockage et l'usage des données à caractère personnel. Elle garantit que tout traitement, sous quelque forme que ce soit, respecte les libertés et droits fondamentaux des personnes physiques ; Elle prend également en compte les prérogatives de l'Etat, les droits et les intérêts des entreprises publiques et privées. Elle veille à ce que les Technologies de l'Information et de la communication ne portent pas atteinte aux libertés individuelles ou publiques, notamment à la vie privée.

2.1 Les données en entreprise :

Les données sont au cœur des priorités stratégiques des entreprises. Elles sont à tous les niveaux, ses sources sont multiples, provenant à la fois des entreprises, des individus, des partenaires publics et privés, voire des machines elles-mêmes. Les données circulent, se reproduisent, se stockent, s'agrègent, se corrèlent ; elles deviennent la matière première de nombreux métiers et la raison d'être de nouveaux marchés, témoignant d'une tendance généralisée qui est la Data Driven Economy (l'économie guidée par les données). Les mutations économiques, stratégiques, politiques et sociales n'en sont qu'à leur début, le déluge des données s'accroissant de manière exponentielle avec le développement récent de nouvelles technologies (objets connectés, machine learning, intelligence artificielle etc.).

Nous sommes aujourd'hui plongés dans l'ère du Big data, de l'interconnexion des données et de leur valorisation. Dans ce contexte Big Data, les données personnelles occupent une place de plus en plus importante. En effet, leurs modes de production, leurs moyens de collecte et d'analyse ont explosé ces dernières années et offrent des potentiels de valorisation gigantesques, mettant notamment l'expérience client au cœur des stratégies. La relation client devient de plus en plus proactive, ce qui permet d'anticiper les besoins, d'adapter les stratégies, les opérations, le retail, etc.

De nombreuses entreprises ont élaboré les premiers modèles fondés sur l'analyse et la revente des données personnelles pour développer leur service. L'économie des données personnelles repose en particulier sur l'évolution de deux modèles qui sont :

- Les modèles bifaces qui se sont construits sur une logique de troc implicite : données personnelles contre service gratuit.

- Les modèles serviciels pour lesquels les données personnelles sont un véritable carburant : grâce à la personnalisation, les services sont plus efficaces et pertinents pour l'utilisateur et bénéficient tant à l'entreprise qu'au client (dans la limite des règles de consentement).

Les données personnelles sont devenues un véritable or noir pour l'économie numérique mais constituent également un risque majeur pour les libertés individuelles, ce qui impacte la manière d'innover. Cela alimente un cercle vicieux. La conciliation est-elle possible ? La protection des données personnelles brime-t-elle nécessairement l'innovation ? Il est parfaitement possible d'innover en faisant du Big Data tout en protégeant la vie privée : cela n'est pas antinomique. En prenant en compte les enjeux de protection des données personnelles le plus en amont possible, dès la conception des technologies, concilier innovation et vie privée devient une démarche non seulement plus responsable mais aussi plus rentable.

Toutes les minutes, l'humanité produit 350 000 Tweets, 15 millions de SMS ; 200 millions de mails ; 250 gigaoctets d'informations sont archivés sur Facebook et 1 740 000 gigaoctects d'informations sont publiés dans le monde. Tous les jours, Google traite plus de 24 peta-octets de données, soit 24 millions de milliards d'octets. En 2013, 1,01 milliards d'objets connectés peuplent la planète. En 2020, nous estimons qu'il y en aura près de 100 milliards. Voici la conséquence logique du poids que le numérique a pris dans notre vie : les données se multiplient à un rythme effréné. Produites par nos ordinateurs, nos téléphones mobiles, nos outils de paiement, mais aussi par les multiples capteurs qui équipent désormais nos entreprises, ces milliards de milliards de données s'accumulent sur les ordinateurs de la planète. Cette démultiplication croissante des sources et des flux de données a généré un accroissement de la production de données structurées, non structurées, semi-structurées, ainsi qu'une baisse des coûts de stockage et d'analyse. Dans cette data-sphère, les données personnelles constituent la matière première essentielle au service du développement de l'économie numérique. Tandis que la stratégie numérique des entreprises oriente de plus en plus les données et leur gouvernance au cœur de leurs priorités, il convient de s'intéresser au cas particulier des données personnelles qui alimentent à elles seules tout un pan de l'économie numérique. De nombreuses sociétés se créent entièrement sur le modèle de la valorisation des données personnelles. Mais lorsqu'il s'agit de créer de la valeur autour des données personnelles, les questions d'éthique et de conformité apparaissent. Comment dès lors préserver la confiance des clients, tout en garantissant le respect de la protection de leurs données ?

2.1.1 Qu'est-ce qu'une donnée personnelle ?

Nous ne pouvons mener une réflexion sur l'économie des données personnelles sans exposer la nature de plus en plus complexe des données personnelles, et la difficulté qu'il y a à saisir dans son ensemble l'immense spectre qu'elles recouvrent.

2.1.1.1 Définition et caractéristiques des données personnelles :

La définition des données personnelles couvre un périmètre très large. Au sens de la loi, C'est toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l'ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou toute autre personne. La notion de donnée personnelle est vaste dans la mesure où elle s'étend à tout ce qui indirectement renvoie à une personne. Est-ce que dans ce contexte, toutes les traces numériques sont des données personnelles ? L'adresse IP a par exemple été considérée comme étant une donnée personnelle, car elle renvoie indirectement à une personne physique ou à un foyer identifié. La donnée personnelle serait-elle finalement presque partout ? Cette complexification de la nature des données personnelles s'explique par le fait que la donnée personnelle est de plus en plus :

- **Protéiforme :**

L'ère numérique marque le passage d'un monde où régnait un seul type de donnée vers un monde où règnent trois types de données : aux données structurées s'ajoutent les données semi-structurées et non-structurées (issues des réseaux sociaux, mobiles, web…). Les systèmes et processus de gestion doivent être agiles et adaptables pour prendre en compte ces caractéristiques de la donnée, en général, et d'autant plus lorsque des données personnelles se cachent derrière ces catégories. Il est à noter que les données personnelles sont classées en deux catégories distinctes :

- ✓ Les données personnelles identifiantes : ce sont les données rattachées directement à l'identité d'une personne. Ce sont généralement le nom, l'adresse, l'e-mail, la situation familiale, ou encore toutes les données ou fichiers permettant d'identifier indirectement une personne, via par exemple un numéro d'identification, une adresse IP.
- ✓ Les données comportementales : ces données sont rattachées à l'ensemble des comportements d'un individu, collectées via le suivi de ses navigations, mettant en exergue ses comportements d'achats ce qui permet, par exemple, pour un retailer (détaillant) d'affiner le profil d'une personne, surtout si ces données comportementales

sont croisées avec des données personnelles identifiantes. En cernant mieux les centres d'intérêt d'un individu et ses préférences, il est possible d'optimiser son parcours d'achat et de lui proposer des offres personnalisées. Ainsi grâce aux données comportementales, les analyses prédictives permettent d'anticiper les types de produits ou de services qui correspondraient le mieux à tel ou tel profil ou à telle ou telle zone géographique. Pour expliquer concrètement la différence entre données personnelles et données comportementales, voici un scénario illustratif : « Mouhamed, père de deux enfants domicilié aux Almadies, se renseigne sur Internet à propos de l'achat d'une nouvelle voiture. Grâce aux sites consultés, nous allons pouvoir lui proposer des essais. Qu'est-ce qui relève des données personnelles ? Il s'agit de son nom, du fait qu'il ait deux enfants rattachés à son foyer et qu'il habite aux Almadies. En termes de données comportementales, nous savons que Mouhamed est prêt à utiliser le web dans sa démarche d'achat, qu'il envisage l'achat d'une nouvelle voiture et qu'il dispose d'un revenu plutôt élevé en raison des marques qui l'intéressent. À partir de toutes ces données, il devient possible d'en déduire que Mouhamed pourrait avoir une propension à acheter plutôt une grosse berline, car il habite dans une commune à fort pouvoir d'achat et qu'il a une famille de deux enfants ».

- **Relative :**

La donnée personnelle est nécessairement liée au référentiel culturel des individus et à la réglementation en vigueur dans chaque pays. C'est un aspect essentiel à prendre en compte quand une société s'adresse à un marché international. Nous pouvons questionner trois perceptions relatives de la donnée personnelle qui impliquent trois approches différentes de la problématique :

- ✓ Du point de vue de l'entreprise : la donnée personnelle a une valeur stratégique et marchande. Elle permet de développer ou d'améliorer les modèles serviciels, d'enrichir l'expérience client, d'être analysée à des fins décisionnelles, d'opérationnalisation, de revente etc. Chaque entreprise fait donc un travail de définition en contexte, en rapport avec le business qu'elle souhaite développer.
- ✓ Du point de vue du client : ses données personnelles sont une émanation de sa personnalité et de sa vie privée, une trace de ses comportements. La confiance qu'il accorde dans les services numériques est fragile si la transparence, les finalités de traitement et les conditions de consentement ne sont pas claires.
- ✓ Du point de vue juridique : le statut juridique de la donnée personnelle permet-il de faire face aux tensions qui existent entre la protection des personnes et les besoins du marché

d'utiliser leurs données pour développer de nouveaux services ? Un Code de la Donnée est-il souhaitable pour prendre en compte les enjeux de la société du XXIème siècle, tout comme l'on a créé un Code de la Propriété Intellectuelle au XXème siècle ?

- **Ouverte :**

La CDP, dans ses dispositions générales relatives à la protection des données à caractère personnel, a recueilli les avis d'experts sur ce sujet. Selon eux :

- ✓ La donnée personnelle offre une vision fermée de la donnée. Or, aujourd'hui, ces données sont ouvertes, elles circulent et se partagent en permanence. La notion même de donnée personnelle ne correspond plus à la réalité. Parler de données personnelles n'a plus de sens, il faudrait plutôt parler de données relationnelles, transactionnelles puisque les données circulent en permanence et qu'il est possible de déduire des informations personnelles à partir de données non personnelles. Le véritable enjeu se trouve dans l'interopérabilité des données.
- ✓ La principale difficulté aujourd'hui est de pouvoir identifier les traitements sensibles et non pas uniquement de sécuriser les données personnelles en tant qu'entité propre.

Figure 1 : Données personnelles

2.1.1.2 Les sources de données personnelles :

Le nouveau paysage de données qui nous entoure est avant tout caractérisé par une grande diversité de la nature des données et de leurs sources : « données transactionnelles, données collaboratives, données issues des systèmes de gestion, registres officiels, médias sociaux, données issues de capteurs et objets connectés, traces numériques, etc. ». Les données personnelles proviennent d'une part des individus eux-mêmes sur internet : données déclaratives, questionnaires, inscriptions en ligne, mais elles s'étendent bien au-delà de cette sphère déclarative. Les hommes ne sont plus les seuls producteurs de données, car les machines en produisent également via différents types de capteurs ou d'objets connectés et qui révèlent parfois plus d'informations personnelles grâce aux techniques de data mining, capables de corréler des données de manière informelle et d'en tirer de nouvelles informations. Par exemple, les voitures connectées dotées de systèmes de machine learning permettent d'analyser des styles de conduites particuliers (sportifs, familial) : ces données de type comportemental sont utiles à la compréhension des usages et permettent via l'analyse prédictive d'anticiper les besoins et de mieux organiser le merchandising. On le voit bien, les modes de production des données personnelles se complexifient avec l'évolution technologique qui enrichit considérablement la nature même des données personnelles, qui ne sont plus seulement liées à l'identité officielle d'un individu mais qui s'étendent à ses habitudes (de navigation, d'achat), à ses parcours d'achats en magasin via la pratique du clienteling, qui consiste à récolter via le Wi-Fi, les données des clients sur leur Smartphone ou en ligne, etc. D'autre part, la façon dont les données sont produites n'est pas toujours, pour leurs auteurs, consciente ou volontaire, et pourtant toutes les traces numériques issues de leurs requêtes sur les moteurs de recherches, tous leurs clics, parcours de navigation ou l'activation de la géolocalisation génèrent autant de données, qui peuvent être ou non associées à une identité physique, via l'adresse IP notamment. La part d'activité de l'individu est considérable dans l'économie numérique. Le digital labor (travail digital) par exemple est un mode de production, une ressource dont les entreprises de l'internet jouissent naturellement en échange de l'‘accès gratuit de l'internaute à un service. Le digital labor est l'ensemble des activités des usagers des plates-formes sociales, des sites web et des applications mobiles. Cela concerne non seulement la publication de contenus générés par les utilisateurs (des photos, des vidéos, des textes), mais aussi toute forme de jeu, de navigation, de bavardage en ligne qui ne serait pas reconnaissable formellement en tant que travail, et qui pourtant produit de la valeur pour les entreprises.

Dans ce contexte, il faut souligner que l'essor des données non structurées (textes, images, requêtes sur les moteurs de recherches etc.) est un phénomène récent qui découle du perfectionnement des outils d'analyse à partir des réseaux sociaux et des navigateurs internet. Ces données non structurées amènent à une compréhension plus précise des comportements des internautes et se révèlent très utiles pour le marketing ou la stratégie d'une entreprise. « Il lui [l'entreprise] est difficile d'accéder aux réclamations que traite le service clients de son principal concurrent ; à l'inverse, il est relativement aisé et tout à fait légal d'enregistrer puis d'analyser tous les tweets, les articles de blogs, les messages Facebook qui parlent des produits dudit concurrent ! ». Ces données non structurées sont une véritable mine d'or pour les entreprises. Sans oublier un autre atout majeur : elles existent sous forme de flux et sont donc nécessairement toujours à jour.

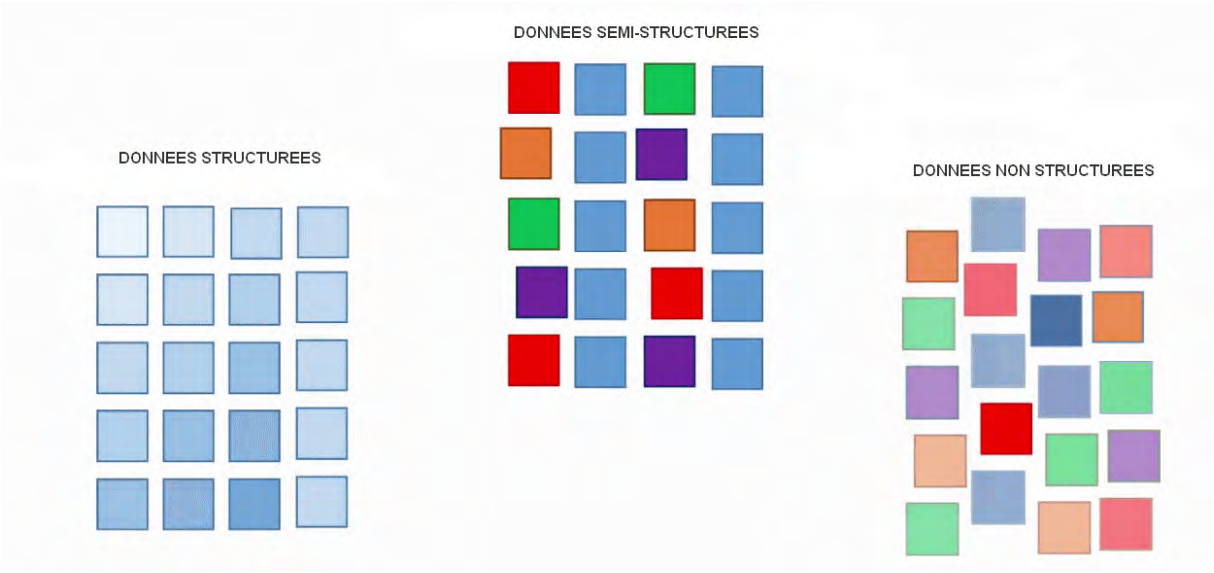

Figure 2 : Structure des données

2.1.2 La valorisation des données personnelles :

Dans le monde numérique, la valorisation des données personnelles ne se limite plus au stockage et à la gestion de fichiers clients, elle n'a aujourd'hui de sens que dans la circulation et l'interaction des données avec tout un écosystème qui peut être interne ou externe à l'entreprise. Cela ne va pas sans poser de nouvelles questions pour les régulateurs. La CDP a en effet soulevé ce nouvel enjeu caractérisant le Big Data, qui est l'interopérabilité des données. Si avec la naissance de la CDP, les enjeux étaient le recueil de données pour de mauvais usages, aujourd'hui c'est l'interopérabilité qui est la nouvelle question centrale. Dans ce contexte Big Data, les données personnelles et leur valorisation prennent une importance croissante. D'ici

2022, le marché des données personnelles représentera une valeur économique de mille milliards d'euros. D'après les prévisions d'IBM (International Business Machines Corporation), d'ici 5 à 10 ans la plus grosse partie des données viendra non pas des usages d'internet mais directement de l'usage des objets (Internet des objets), qui encadrent notre quotidien. Ces tendances économiques et technologiques témoignent d'un avenir prometteur pour l'économie des données personnelles, mais celle-ci ne se fera pas sans le concours des consommateurs/clients qui prennent une part de plus en plus importante dans les processus de valorisation.

2.1.2.1 Les potentiels de valorisation des données personnelles :

Les grandes entreprises ont progressivement pris conscience du potentiel de création de valeur que leur apportait l'usage des données ciblées, notamment via les technologies qui sous-tendent le Big Data, appliquées en particulier à la masse croissante de données qu'elles peuvent mobiliser sur leurs clients. Mieux connaître ses clients, comprendre leurs comportements et leurs attentes, anticiper leurs réactions permet de les fidéliser et de leur proposer les offres personnalisées les mieux adaptées. C'est un enjeu majeur pour toutes les entreprises, enjeu souvent inscrit au premier rang dans leur stratégie. Parallèlement à la croissance régulière des données internes des entreprises, corrélées plus ou moins à la croissance et à la diversité des activités des grands groupes, la montée en puissance d'acteurs du Web a révélé le potentiel immense des données externes à l'entreprise. Cette masse jugée inqualifiable et inexploitable jusqu'aux années 2000 constitue la base de recherches des opportunités de demain. Grâce aux moyens et outils de mesures disponibles pour traiter ces Big Data, les données personnelles se révèlent être des actifs inédits et précieux pour les entreprises dans des domaines variés.

2.1.2.1.1 Stratégiques :

Les modèles de valorisation des données personnelles ouvrent de plus en plus la voie aux alliances stratégiques, à la co-création de services et de produits, au partage de données avec des entreprises tierces et en BtoB. Les secteurs de l'automobile et de l'assurance sont par exemple amenés à travailler ensemble sur la voiture connectée par l'intermédiation de plateformes numériques. C'est aussi le pari qu'à fait Nike en industrialisant un produit (des chaussures) avec des services associés, c'est-à-dire la création d'une plateforme qui collecte, centralise et met à disposition des utilisateurs les données. C'est cet atout stratégique qui a fait la différence et lui a accordé un avantage concurrentiel sans précédent, avec au cœur, la donnée personnelle comme actif stratégique.

2.1.2.1.2 Opérationnels :

Via l'anonymisation de données, l'exploitation des données personnelles dans un contexte Big Data permet d'optimiser des processus opérationnels. C'est ainsi que procèdent de nombreux services de transport qui mesurent les flux de passagers après avoir anonymisé les données pour adapter leurs services en fonction de la connaissance des passages les plus fréquentés, ou les plus désertés à certaines tranches horaires permet d'adapter, parfois en temps réel, les services de surveillance, de régulation des flux, les ouvertures des guichets d'informations, des points de vente etc.

2.1.2.1.3 Recherche et développement :

Il est courant que l'entreprise crée de la valeur sur les données via l'expérimentation, et donc selon un usage non défini à l'avance. Or, un des principes fondamentaux de la protection des données personnelles est d'informer la personne concernée de la finalité du traitement au moment de la collecte de ses données afin d'en obtenir un consentement éclairé. Cette finalité n'est pas toujours simple à définir à l'avance dans le cadre de l'innovation ou de la Recherche et Développement. Le recours à une définition de cette finalité de manière relativement générique permet de se laisser une marge de manœuvre suffisante pour valoriser au mieux les expérimentations. De plus, tant que le contexte n'est pas lié au business, les données personnelles peuvent faire l'objet d'analyses réalisées en silos, et permettre par exemple d'améliorer la qualité d'autres données, d'affiner un modèle algorithmique, et ainsi de perfectionner les savoir-faire internes des entreprises. Certaines méthodologies Big Data permettent en effet d'extraire des modèles pertinents sur la base de données personnelles. Les modèles prédictifs, fréquents dans les approches Big Data, peuvent ainsi catégoriser/segmenter une base clients sans recourir à l'identification personnelle.

2.1.2.1.4 Marketing :

La personnalisation des services et des produits à des fins marketings est un pilier de l'économie des données personnelles. De nombreuses plateformes Web sont fondées exclusivement sur la vente de retail. L'analyse comportementale peut porter sur des données non-structurées et permettre de développer des modèles prédictifs pour être proactif dans la relation et la connaissance client. De nombreux modèles existent, mais nous pouvons citer en particulier les résultats rendus publics des chercheurs iraniens des universités Azad et Alzahra à Téhéran : ils ont mis au point un algorithme de modélisation par apprentissage semi-automatisé des comportements clients par l'intégration de données non balisées à un classificateur de données balisées.

Les données non balisées sont alors traitées et classifiées par rapport au classificateur initial de données balisées. Un nouveau classificateur est ainsi créé, regroupant les données balisées et celles nouvellement balisées. Ce système permet d'acquérir un meilleur degré de confiance et de précision pour l'évaluation des modèles, notamment des modèles prédictifs. L'usage marketing des données personnelles ne se fera pas cependant sans le concours et le consentement des individus. Selon une enquête menée en février 2014 par SerdaLAB auprès de 533 individus de 15 à 65 ans, 90% des personnes acceptent les pratiques commerciales à partir de leurs données personnelles, à condition d'exprimer au préalable leur consentement et de pouvoir maîtriser les conditions de cette réutilisation des données. Par ailleurs, les données de consommation sont jugées par les trois quarts des répondants comme étant les moins sensibles pour une réutilisation commerciale, tandis que les données de géolocalisation, de navigation internet, des réseaux sociaux, de santé et les données bancaires sont considérées comme étant les plus confidentielles. En outre, les individus acceptent d'être scrutés et analysés en tant que consommateurs, beaucoup moins en tant que citoyens (opinions, réseaux sociaux, géolocalisation).

2.1.3 Anonymisation versus valorisation ?

Comment valoriser une donnée personnelle si celle-ci est anonyme ? Cette question illustre l'opposition fréquente que les entreprises établissent entre protection des données personnelles et valorisation. Il existe pourtant des méthodes qui permettent de rendre les données cohérentes, statistiquement significatives, sans être nécessairement nominatives : c'est ce qui est attendu par les entreprises et cadré par la législation.

Il doit être cependant souligné que l'anonymisation sera chaque jour plus complexe, notamment avec l'émergence du temps réel. Les progrès techniques et la multiplicité des sources des données fragilisent en effet la durabilité de l'anonymisation des données et mettent en cause les investissements qui seraient faits dans ce sens. Il faut notamment prendre garde à la notion de « jeu de données anonymes » car il est toujours possible de le « désanonymiser » dans un contexte Big Data. Un jeu de données anonymes peut donc être de nouveau soumis à la loi informatique. L'anonymisation est quelque chose qui doit être sans cesse révisé dans le temps. Au regard de ces nouvelles complexités, assurer une bonne gestion des données personnelles par l'exercice du droit des personnes, semble une approche beaucoup plus réaliste et économique. Rappelons en effet que l'usage de données personnelles n'est pas interdit, il est juste soumis à la loi informatique. Cela nécessite un consentement éclairé du client, établissant un premier contrat dans cette relation.

2.1.4 Les innovations technologiques : quel avenir pour les données personnelles ?

Certaines innovations technologiques qui s'intègrent peu à peu sur le marché s'orientent de plus en plus vers la quantification et la mesure des activités humaines, du corps, et vont également impacter les modèles décisionnels : Internet des objets, intelligence artificielle, machine to machine. C'est un marché qui confirme la tendance généralisée de collecte de données qui entrent de plein pied dans la sphère intime des individus. Les données personnelles sont-elles finalement driver l'économie numérique ?

La technologie devient de plus en plus miniaturisée et permet de vêtir l'ensemble du corps de capteurs et d'augmenter l'homme. La captation de l'individu et de son environnement ouvre la porte au développement des modèles serviciels, qui seront davantage tournés vers le prédictif. Quoiqu'il en soit, il faut s'attendre à ce que tous les secteurs, toutes les industries soient touchées par cet outillage connecté de l'homme. Les hôpitaux auraient-ils par exemple vocation à se transformer en immense datacenter analysant les données des patients, gérées par un système d'IA, offrant ainsi des suivis personnalisés ? Pour aller un peu loin, la fusion du cerveau et des machines est également un scénario du futur très probable. L'ordinateur va apprendre à ressentir les émotions des personnes avec lesquelles il est en contact. On va vivre une communication différente entre l'homme et les machines et ce bouleversement est pour demain. Des centaines de laboratoires dans le monde travaillent sur ces projets. Ils tentent de faire fusionner le cerveau et les machines. L'interaction homme-machine serait ici à son paroxysme ; l'homme n'existerait plus sans ses outillages technologiques qui l'habillent, le guident, surveillent sa santé, son bien-être, sa performance etc. Les investissements technologiques semblent bien être tournés de plus en plus vers cette personnalisation exacerbée de l'homme et de son augmentation. Quoiqu'il en soit, le défi majeur pour les entreprises et acteurs du numérique sera dans la détermination de la responsabilité qui nécessite autant la compréhension que l'intégration du futur, sans savoir véritablement ce qu'il sera et c'est bien là où se trouve la complexité.

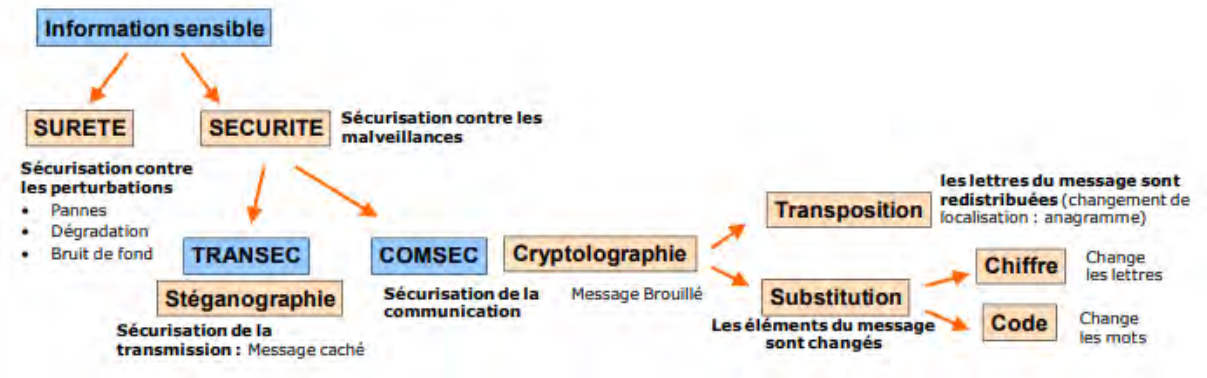

Figure 3 : Données sensibles

2.2 Cadre juridique de la protection des données personnelles :

Chaque société a sa propre culture de la confidentialité, bien que les transactions commerciales exigent que la sécurité des informations soit déterminée par le point d'origine des données. Quel que soit l'endroit où les données sont traitées dans un environnement en réseau mondial, l'entreprise qui collecte à l'origine les données, est tenue de respecter les obligations de confidentialité, quel que soit l'endroit où les données circulent. Les attentes particulières en matière de confidentialité sont donc véritablement locales, tandis que les flux de données sont mondiaux. Cependant, il est difficile de gérer les flux de données transfrontaliers en vertu des lois ou des cadres juridiques d'un pays. Le défi est donc pour les entreprises informatiques et pour respecter les obligations de confidentialité et de sécurité de l'information lorsque les lois nationales diffèrent.

Avec le développement de l'informatique et de ses applications, le domaine traditionnel de la vie privée s'enrichit chaque jour de nouveaux éléments. Partie intégrante de ces éléments, les données à caractère personnel se révèlent être des ressources très convoitées. Leur traitement doit se dérouler dans le respect des droits, des libertés fondamentales, de la dignité des personnes physiques. De ce fait, la législation sur les données à caractère personnel s'avère un instrument de protection générale à l'égard de ces droits et libertés de la personne. Malgré le démarrage de l'Intranet gouvernemental, le développement du recours à l'informatique dans l'administration, dans les entreprises privées et son utilisation par les personnes, la numérisation du fichier électoral et de la carte d'identité nationale, entraînant ainsi la génération, la collecte et le traitement des données à caractère personnel, le droit positif sénégalais ne fixe pas le cadre et le régime juridique de ces opérations. L'ambition du projet de loi 2008-12 est de combler ce vide juridique. Prenant pour base les principes directeurs pour la réglementation des fichiers

informatisés contenant des données à caractère personnel édictés par l'Assemblée Générale de l'ONU en 1990, les exigences en matière de transfert de données vers des pays tiers et les principes fondamentaux consacrés par la loi d'orientation sur la société de l'information, le présent projet de loi sur la protection des données à caractère personnel offre un autre niveau élevé de protection.

2ème Partie : Cadre conceptuel

Chapitre 3 : Ressource et Identité Numérique en entreprise

La transition numérique n'est pas réductible à son aspect technique. Elle bouleverse l'ensemble des dimensions du travail, depuis ses organisations jusqu'à ses finalités, en passant par les manières de le réaliser et par les conditions dans lesquelles il s'exerce. Elle ouvre des perspectives de transformation sociale des rapports au travail et des organisations de travail sur la base d'un renouvellement des usages, des capacités et des relations, dont les acteurs sociaux commencent à se saisir comme enjeux de régulation collective.

Le développement des nouvelles Technologies de l'Information et de la Communication a généré, outre les bouleversements économiques que nous connaissons, de nouveaux usages professionnels, souvent peu maîtrisés et mal encadrés. On constate que les TIC ont mis en évidence par leur capacité à exacerber certaines dérives de nombreuses lacunes du droit du travail : forfait jours, prise en compte de la charge et du lieu de travail, télétravail, sécurité et contrôle, etc. Il est donc nécessaire, pour faire des TIC une source de progrès, aussi bien pour l'employé que pour l'entreprise, d'établir de nouvelles protections collectives et individuelles. Celles-ci devront être à-même de poser des mesures capables notamment de recréer une frontière entre vie privée et vie professionnelle, et partant, d'adapter les protections et endiguer les dérives citées. La digitalisation a quelque chose d'inéluctable et chacun doit s'approprier ce nouvel espace, à la fois pour faire bénéficier aux employés des opportunités inhérentes à ces nouvelles technologies mais aussi pour les prévenir des risques.

3.1 Les ressources Numériques en entreprise

Les ressources numériques sont diverses et regroupent entre autres, les applications, les bases de données et les infrastructures informatiques. C'est un ensemble de ressources qu'il convient de gérer de manière efficiente, afin de s'assurer qu'elles sont sources de performance. Les ressources, ce sont aussi les compétences qui permettent aux acteurs de l'entreprise de tirer parti de toutes les potentialités du numérique pour développer leur modèle d'affaires, leurs activités et leurs offres de valeur. Le développement de ces compétences numériques constitue la clé essentielle permettant à l'entreprise numérique de se déployer de manière pertinente. Selon Roger Martin qui a bien résumé l'enjeu de l'intégration des nouvelles compétences. En le paraphrasant, ses réflexions peuvent être adaptées à l'entreprise numérique : aujourd'hui, pour un acteur métier dans l'entreprise, il n'est pas suffisant de comprendre les systèmes d'information, il faut aussi devenir soit informaticien, soit chef de projet numérique.

Figure 4 : Ressource Numérique

3.1.1 Principaux avantages des ressources numériques :

Qu'il s'agisse des données de l'entreprise, le site web, les applications ou des vidéos réalisées lors des événements de l'entreprise, les ressources numériques sont des éléments indispensables, sans lesquels l'organisation ne peut pas mener à bien ses missions. Les entreprises ont besoin de ressources numériques pour faire connaître leur marque et instaurer l'identité visuelle de leurs produits ou services. La forte visibilité des ressources imprimées ou diffusées sur les réseaux sociaux, les applications et les sites web leur confère une grande valeur. Ces dernières années, beaucoup d'organisations confrontées à des quantités croissantes de ressources numériques ont adopté des systèmes de gestion de ces ressources. Leurs motivations sont multiples et parfois très simples.

- Les logiciels de gestion des ressources numériques s'intègrent directement aux logiciels de création et en optimisent les fonctionnalités, simplifient les processus de travail et améliorent la productivité.
- Pour dynamiser la productivité, un logiciel de gestion des ressources digitales (DAM) de qualité obéit à une logique intuitive et est mis en place rapidement, sans qu'il soit nécessaire de faire sans cesse appel à l'assistance technique.
- Les ressources gérées par un système de DAM peuvent être partagées plus facilement, ce qui garantit un fonctionnement optimal.
- La gestion des ressources numériques simplifie les échanges des fichiers au sein des équipes, quelle que soit leur taille.

3.1.2 Les systèmes d'information au cœur des ressources numériques :

Dans un contexte de forte transformation de l'entreprise, le système d'information prend une place de plus en plus stratégique dans la chaîne de valeur : il est désormais présent dans tous les métiers de l'entreprise, et au-delà dans le cadre de l'entreprise numérique (interactions avec les clients, les fournisseurs et autres parties prenantes). Schématiquement, un système d'information repose sur trois piliers :

- des applications pour organiser les processus des métiers,
- des bases de données pour stocker et mettre en forme les données,
- des infrastructures pour traiter l'information et assurer les échanges.

Le SI est un ensemble organisé de ressources techniques, organisationnelles et humaines, requises par le traitement des informations nécessaires à la stratégie et aux métiers de l'entreprise.

Le SI comporte deux dimensions : celle de l'organisation qui se transforme, entreprend, communique et enregistre les informations, et celle du système informatique, objet artificiel conçu par l'homme qui permet l'acquisition, le traitement, le stockage, la transmission et la restitution des informations au service de la gestion de l'entreprise. Pour l'entreprise numérique, le SI est le facteur critique d'efficience opérationnelle.

3.1.2.1 Les applications

La mise en œuvre d'applications répond à la problématique d'évolution de l'entreprise vers l'entreprise numérique : elles ne peuvent plus être considérées comme accessoires par les métiers. Leur place est au cœur des activités et elles doivent être intégrées en première intention par les métiers pour maîtriser, puis optimiser, les processus en termes de qualité et d'efficience. Ces applications deviennent, comme nous l'avons évoqué, les solutions de l'entreprise numérique (PLM, MRP, CRM, ERP).

3.1.2.2 Les bases de données

Avec l'explosion de la création des contenus, plus ou moins structurés, les bases de données acquièrent une importance toute particulière comme piliers du système d'information. C'est l'un des domaines qui fait l'objet de recherches, en lien avec les technologies de réseaux. Par exemple l'Advanced Database Research Group (ADRG) étudie l'interopérabilité entre les systèmes de bases de données hétérogènes et définit des échanges électroniques de données transparents entre les différents systèmes de bases de données. Cette solution évite d'imposer des systèmes de bases de données uniformes et permet une plus grande flexibilité. IBM

Research a été l'un des premiers à se lancer dans la recherche sur des méthodes efficaces d'accès aux données semi-structurées et non structurées.

3.1.3 L'importance croissante des infrastructures informatiques et des services associés

3.1.3.1 le cloud Computing

La tendance la plus marquante actuellement est celle du cloud computing (l'informatique en nuage) et des logiciels en tant que services (Software as a Service, ou SaaS) comme cibles privilégiées des investissements technologiques. Les services logiciels traditionnels sont progressivement transférés sur le réseau (Internet) et proposés sous forme de services. Par exemple, les solutions de CRM sont de moins en moins déployées à l'intérieur du réseau informatique des organisations, mais plutôt hébergées par une entreprise tierce qui offre un accès par Internet à la demande. On peut comparer cette évolution à celle des messageries individuelles, qui sont à présent accessibles depuis n'importe quel ordinateur à l'aide d'un navigateur Internet. Cette approche permet de contourner les investissements initiaux significatifs liés à l'achat des logiciels et des matériels. Différents fournisseurs proposent des produits et des services qui modifient la façon de travailler au quotidien et influencent le mode de fonctionnement des entreprises.

Faire plus vite, moins cher, en optimisant les ressources, tel est le message des dirigeants. Les systèmes d'information, en tant que système nerveux de l'entreprise, doivent aider le management dans la réalisation de cet objectif. Le cloud computing est susceptible d'avoir un impact profond sur la stratégie de l'entreprise et sur ses métiers. C'est cet impact qu'il convient d'évaluer en termes de valeur, de risques et de pratiques. L'émergence du cloud computing et des services associés constitue une mutation qui se traduit par des modèles économiques différents et des offres nouvelles ayant un impact important sur l'écosystème des services d'information des entreprises.

Le cloud computing est une solution à combiner aux solutions SI existantes. La fonction SI a un rôle d'intégrateur ultime avec les processus métiers et les autres solutions constituant le patrimoine applicatif de l'entreprise étendue. Les offres de cloud computing doivent donc être interopérables, réversibles et reposer sur des standards ouverts. Ils doivent être aussi source d'innovation pour les entreprises, en termes de financement, de sourcing, d'architecture et surtout de services différenciés.

Figure 5 : Cloud Computing

3.1.3.2 Le remplacement des ordinateurs portables par les smartphones et les tablettes :

Le nombre de smartphones en circulation dans le monde sera presque équivalent à celui des micro-ordinateurs. On le voit, les nouvelles générations de terminaux nomades vont imposer une reconfiguration des systèmes d'information avec une rapidité qui n'a pas toujours été anticipée par les entreprises. Les nouveaux usages nécessitent de plus en plus des applications mobiles, c'est-à-dire compatibles avec une utilisation par smartphone.

La porosité du système d'information, l'effacement des frontières entre la sphère privée et professionnelle, la diffusion rapide des applications à la demande favorisent l'ancrage de nombreux services et produits numériques dans les systèmes d'information. Ceux-ci deviennent des éléments indispensables de cohérence et de flexibilité opérationnelle. Garantir une telle réactivité doit figurer en tête de l'agenda des entreprises : l'excellence opérationnelle conditionne la création de valeur. La gestion des ressources numériques doit désormais non seulement répondre aux exigences des utilisateurs internes, mais également à celles des clients et partenaires de l'entreprise numérique. Elle reste indissociable de la protection et de la valorisation du patrimoine informationnel des entreprises.

3.1.4 L'archivage numérique pour préserver le patrimoine de l'entreprise :

L'archivage remonte dans les préoccupations des directions générales, pour plusieurs raisons. D'abord, l'explosion des volumes de données induit, de fait, des interrogations sur la manière de stocker les données (approche quantitative), de les restituer et de les mettre en forme (approche qualitative). Ensuite, l'évolution des technologies impose d'inclure l'archivage dans les problématiques de l'entreprise numérique, notamment parce qu'il faut conserver les données dans de bonnes conditions de pérennité. Enfin, l'évolution du contexte réglementaire pousse

également à structurer la réflexion autour de l'archivage. Quatre besoins doivent être satisfaits par l'archivage : garantir la sécurité (disponibilité, intégrité des données, confidentialité, traçabilité), répondre aux exigences légales (pour la conservation et la recherche obligatoires de documents), s'adapter à l'évolution technologique et faciliter la vie des utilisateurs en leur proposant des outils d'accès aux informations.

La problématique de l'archivage électronique ne se limite pas à une simple dématérialisation des techniques d'archivage traditionnelles. Outre l'influence des nouvelles obligations, ce nouveau type d'archivage doit être considéré très en amont dans la chaîne de valeur de l'information, d'où la volonté de prendre en compte l'ensemble du cycle de vie de la donnée. C'est le patrimoine informationnel qui est en jeu. Celui-ci peut se définir comme l'ensemble des données et des connaissances, protégées ou non, valorisables ou historiques d'une personne physique ou morale. Il s'agit donc d'assurer la protection et la valorisation de l'information.

3.1.5 Le développement d'un contrôle de gestion adapté :

L'extension des domaines applicatifs, des nouveaux besoins et du nombre d'utilisateurs des systèmes d'information, donc des budgets informatiques, a renforcé le rôle du contrôle de gestion comme bonne pratique de pilotage des services. En pénétrant toujours plus profondément dans la chaîne de valeur de l'entreprise numérique, les ressources informatiques deviennent un élément clé de la rentabilité opérationnelle et de l'élaboration des catalogues de revenus.

3.1.5.1 La recherche permanente d'efficience et de productivité

Ces dernières années, des structures organisationnelles intégrées à la fonction SI ont été créées afin de maîtriser et expliquer les coûts. L'évolution de ce contrôle de gestion s'est alignée sur la diffusion de l'informatique dans l'entreprise avec la recherche des bénéfices métiers pour moteur principal. Cette recherche permanente d'efficience et de productivité s'applique encore plus à l'entreprise numérique, dès lors que la création de valeur par les services et les biens immatériels devient plus importante à mesurer.

L'entreprise numérique apporte une couche supplémentaire de complexité pour les fonctions de contrôle de gestion. Historiquement, l'automatisation des processus et des chaînes de valeur a entraîné des gains relativement faciles à calculer, avec la notion de retour sur investissement. L'extension des systèmes informatiques et la mise en œuvre d'applications multiples ont éclaté les investissements vers les différents métiers de l'entreprise. Les gains associés sont moins faciles à mettre en évidence. Les directions informatiques et métiers ont alors besoin de s'appuyer sur un contrôle de gestion informatique dédié et adapté. Avec les grands applicatifs

tels que les ERP, la complexité s'est encore accrue, puisque toute l'entreprise est concernée. Le contrôle de gestion informatique doit poursuivre le développement des bonnes pratiques, consolider les règles d'analyse de la valeur ajoutée pour les métiers et concevoir les méthodes pour évaluer les coûts de revient des services numériques.

3.1.5.2 Le modèle économique interne des entités de services partagés :

La montée en puissance de l'externalisation et des centres de services partagés (CSP) introduit aussi de nouvelles considérations économiques. La complexité des organisations rend la lisibilité des gains inversement proportionnelle à celle des coûts engagés et les directions générales demandent des efforts d'explication dès que leur perception des gains devient inférieure à celle qu'elles ont des coûts. Dans cet univers, le rôle du contrôle de gestion renforce encore son importance. Il doit rendre les ressources des entités de services internes plus transparentes en fournissant une aide à la justification économique des projets, à la décision et au dialogue avec les directions métiers. Les centres de services partagés constituent une tendance managériale qui se développe et des entreprises ont d'ores et déjà adopté ce modèle dans des secteurs variés (banque, assurance, services). C'est une forme d'organisation qui semble constituer une tendance de fond pour les fonctions support (RH, finances, achats). Plusieurs facteurs sont à l'origine du développement des centres de services partagés : tout d'abord, le souhait de mutualiser les services fonctionnels ; ensuite, la volonté de créer des cultures communes via la standardisation des processus, des architectures et des méthodes ; enfin, la volonté de concentrer les savoir-faire et de mieux responsabiliser chaque acteur. Ce modèle est parfaitement compatible avec d'autres modèles de sourcing telles que l'infogérance sélective ou les pratiques d'offshore. Le CSP permet de professionnaliser les services et constitue un levier de standardisation et de transparence sur les coûts au sein des entreprises. C'est un nouveau modèle d'organisation dont la mise en œuvre est facilitée par la numérisation des activités, en particulier pour opérer à distance. C'est aussi une nouvelle philosophie et un nouveau mode de management pour l'entreprise numérique.

3.2 L'évolution du Numérique :

Pour étudier l'influence du numérique sur le travail, nous nous sommes appuyés sur le champ de la littérature existante en proposant une présentation du numérique et de son évolution au sein des organisations, les effets constatés du numérique sur le travail à ce jour. Comme le travail ne peut s'analyser en dehors d'une organisation (comprenant structures, managers et individus), l'influence du numérique sur le travail s'analyse dans l'usage que les individus en

ont dans le sens où on ne peut dissocier l'individu de la technologie pour comprendre son influence ce qui explique la mobilisation du concept de socio-matérialité.

Le numérique interagit dans le monde du travail à trois niveaux de l'espace, que ce soit dans l'espace-temps en lien avec le respect de la vie professionnelle et la vie personnelle, l'espace-lieu en lien avec les mobilités et le nomadisme et enfin l'espace-territoire en lien avec les spécificités des territoires et du business associé. On complète en spécifiant que l'espace-temps est différent car aujourd'hui les discours managériaux prônent l'action rapide, l'improvisation, la prise de risque, un rapport à l'espace modifié par des interactions se faisant à distance, modifiant les perceptions, offrant des prises de décision rapide et augmentant le volume des échanges et des flux d'informations.

3.2.1 La transformation numérique :

On définit la transformation numérique comme une manière différente de produire de la valeur, d'interagir avec l'extérieur et de déployer des projets. Autrement dit, faire appel au numérique, à des leviers numériques, demande de penser autrement l'informatique, l'organisation, la structure. Il s'agit d'identifier les usages internes, les règles existantes, identifier l'explicite comme le tacite, et proposer des méthodes dites agiles allant parfois dans le sens opposé des usages existants. Ce phénomène vient bouleverser les postures au sein des grandes organisations dans lesquelles on retrouve des schémas d'interventions liés aux usages, aux règles tacites, à la culture, aux structures définies faisant sens auprès des individus, leur permettant de justifier leurs actions. Le fonctionnement en silos des organisations, le contrôle, le cloisonnement sont autant de freins à l'innovation. Ce qui pose la question aux organisations d'ajuster leurs configurations organisationnelles de type bureaucratique à un type adhocratique. La question du contrôle et de la confiance se pose également. Car ce qui rassure une organisation réside bien dans la reproduction des mêmes schémas d'interventions, de l'homogénéité des comportements des individus, tous ralliés ou reliés autour de la culture de l'entreprise. Dans le cadre de la transformation numérique, on vient questionner le sens donné au produit, au service, au nouvel usage et questionner ainsi l'intelligence collective, les valeurs, les attitudes à adopter. La transformation numérique désigne le processus qui permet aux entreprises d'intégrer toutes les technologies digitales disponibles au sein de leurs activités.

3.2.2 Des TICs au Big Data :

Ces dernières années, le nombre de données a littéralement explosé dans les activités des entreprises. Les technologies qui permettent l'exploitation de ces données au volume important

présentent quelques points particuliers, notamment pour permettre la collecte et la fouille dans ces données de grand volume. Ce phénomène de données massives ou big data, amène les organisations à se positionner sur l'exploitation de tels volumes d'informations et notamment à mettre en place des processus organisationnels pour les aider à maîtriser cette pléthore d'informations à des fins d'intelligence pour la décision et l'action. Ainsi, face à l'ampleur de ce phénomène, lié notamment à la prolifération des données de l'entreprise, leur croissance exponentielle et les problèmes de repérage, d'accès, de gestion et de traitement de ces données, un certain nombre d'organisations, entre autres des entreprises du domaine privé, ont pris conscience de l'exploitation de ces données massives.
Le big data correspond à une évolution de la business intelligence qui repose sur des entrepôts de données limités en taille (quelques téraoctets) et gérant difficilement des données non structurées et des analyses en temps réel. L'avènement du big data ouvre une nouvelle ère technologique qui offre des architectures et des infrastructures évoluées qui permettent en particulier des analyses sophistiquées, prenant en compte ces nouvelles données intégrées à l'écosystème de l'entreprise

Les outils numériques interviennent dans différentes dimensions du travail, que ce soit sur le fond ou sur la forme, en modélisant des tâches, en rationnalisant des activités, en véhiculant une culture organisationnelle, en proposant de nouveaux schémas de coopération et/ou d'organisation. On peut compléter ces définitions en constatant que le numérique peut être assimilé à un « pharmakon », à savoir un poison et un remède. En intervenant dans tous les secteurs d'activités et dans le quotidien des individus, il devient une nouvelle forme de savoir, une nouvelle forme d'écriture, produit par l'intermédiaire d'outils ayant la capacité de lire des données écrites et d'en produire de nouvelles, et enfin les outils utilisés par des entreprises à envergure mondiale ayant une faible ancienneté sur le marché.

3.2.3 L'évolution des outils numériques dans les organisations :

Au regard des définitions proposées, nous constatons que l'évolution des outils numériques et leur mise en œuvre au sein des organisations répond à une problématique d'ordre économique. Leur présence s'est fait ressentir dans les années 50 avec l'automatisation puis s'est développée avec l'introduction des progiciels de gestion intégrés et enfin s'est décentralisée au niveau individuel avec la démocratisation d'internet. Nous sommes arrivés à la virtualisation des systèmes d'information avec le cloud computing, autrement dit l'informatique dans les nuages. Le déploiement des technologies d'information et de communication correspond aux choix stratégiques et organisationnels des entreprises, stratégies en lien avec les configurations

organisationnelles leur permettant de répondre à la financiarisation de l'économie. Ce qui répond concrètement aux objectifs de rationalisation, de qualité, de transparence, de traçabilité, d'augmentation de la flexibilité. Peu importe la forme de l'outil, que ce soit une boîte mail électronique, une base de données, ce que recherche avant tout une organisation, ce sont les services rendus par ces technologies, répondant aux objectifs ci-dessus. Par exemple, une base de données, permettra à toutes les filiales de sortir le même format de reporting répondant ainsi à un autre objectif celui de la qualité mais également de la transparence et de la traçabilité. Avec l'arrivée du cloud computing, les outils sont mobiles, ne subissent plus la contrainte du lieu physique et offre la possibilité d'accès aux données via des plateformes ou des logiciels d'application à tout moment et à n'importe quel endroit. Nous ne pouvons que constater la démultiplication des outils et leur niveau de complexification, ce qui n'est pas sans effet sur le travail.

3.2.4 Les défis du numérique :

A l'ère du numérique, plusieurs défis sont à relever. Successivement, nous sommes passés de l'invention de l'écriture à la création de l'imprimerie, diffusant l'information d'un support papier à un support internet où la création de l'information n'appartient plus à une certaine catégorie d'auteurs mais où chaque individu peut via internet devenir créateur et lecteur d'informations. Ce que nous entendons par révolution digitale fait référence au progrès technique qui a permis le nombre croissant de partages de données, d'informations devenues numérisées. La loi de Moore, (nom du cofondateur d'Intel qui l'a observée pour la première fois en 1965, fait référence au nombre de microprocesseurs sur une puce électronique qui double tous les deux ans) illustre la vitesse à laquelle la technologie progresse. La matière première de cette révolution numérique est caractérisée par la donnée numérique, donnée située et contextuelle, apparaissant dans un échange ou dans une situation. Certaines règles sont à respecter pour légitimer son utilisation à savoir : « la donnée doit être collectée dans un but précis, l'information doit être en lien avec l'objectif visé, la donnée doit disparaitre quand la raison de la collecte disparait elle aussi, et elle ne peut être collectée qu'avec accord de son créateur ». Ces données sont traitées par des algorithmes dans l'objectif de prédire des comportements, de définir des usages, qui une fois modélisées seront sur le marché. Le nombre croissant de données, autrement dit le « big data » ou « méga-données », traité par des algorithmes, sert également les organisations dans leur prise de décisions. En d'autres termes, analyser les données dans une logique descriptive permet de visualiser les données, dans une logique prédictive permet de prédire un comportement mais dans une logique prescriptive cela

demandera une analyse de données en temps réel offrant une prise de décision rapide. D'autres questions gravitent autour de la gestion des données comme leur protection et l'échelle liée à cette protection (individuelle, nationale ou mondiale). Mais également des questions liées à l'emploi, au monde du travail, à la réalisation des tâches répétitives assurées par des outils numériques, à la question de la pérennité du statut du salariat et à l'évolution du droit du travail qui répond aux conséquences du numérique dans les évolutions des usages. On évoque une évolution du travail vers de l'artisanat plutôt qu'un travail à la chaine, sous-entendu répondre un besoin précis, faire de l'unicité au moment où le besoin se créée. Le numérique est une source d'agilité dans le sens où il permet d'aller plus vite dans l'accès à l'information et la prise de décisions, dans la création d'emploi à forte valeur ajoutée mais est aussi une source de fragilité dans le sens où la croissance ne s'accompagne pas forcément de création d'emplois pour certaines tâches liées à la collecte des données.

3.3 L'usage des ressources Numériques en entreprise :

Chacun peut l'éprouver tous les jours, l'usage des technologies numériques a des effets sur l'organisation, le management, la culture, le rapport au travail, les échanges, les compétences de l'ensemble des acteurs de la chaîne de valeur de l'entreprise, mais aussi chez ses fournisseurs et clients. La nature des effets des outils numériques et de leur usage sur les conditions de travail est ambivalente. Si leur pratique peut offrir aux employés plus de flexibilité, d'autonomie et de coopération, elle peut aussi générer son lot de problèmes, d'autant plus réels qu'ils sont difficiles à identifier et donc à résoudre : surcharge informative, intensification et individualisation du travail, renforcement du contrôle de l'activité, contraintes excessives de réactivité, brouillage des frontières entre vie familiale et vie professionnelle, désintégration des collectifs et désincarnation du management.

3.3.1 Impacts individuels :

En l'absence de régulation, l'usage d'outils numériques peut contribuer à la détérioration des conditions de travail, d'autant que la rapidité et la facilité des échanges via le numérique ont favorisé l'émergence d'une culture de l'urgence et de l'immédiateté. Lorsqu'elle se traduit par une réduction des marges de manœuvre et des capacités d'apprentissage, d'initiative et de reconnaissance pour l'individu, la transition numérique démultiplie les atteintes à la santé des travailleurs (usure professionnelle, risques psychosociaux).

Ces impacts individuels se doublent d'effets plus structurels, moins immédiatement perçus : en permettant de réorganiser les processus de production au-delà des frontières matérielles de l'entreprise, la transition numérique fait voler en éclats le principe d'unité de temps et de lieux

sur lequel se sont construits les cadres de régulation de la relation de travail. La transition numérique induit une dislocation spatiotemporelle des cadres organisationnels. Les frontières de la relation d'emploi et du travail lui-même tendent à se brouiller. De nouvelles relations entre les espaces et les temps sociaux se construisent autour de ces technologies, sans que ces modes de travail soient toujours bien compris, régulés et négociés : télétravail, pratiques nomades, travail en réseau dans des collectifs étendus, coactivité plus ou moins encouragée ou tolérée par l'employeur ou le management.

3.3.2 Approche Organisationnelle :

L'on peut également poser l'hypothèse qu'en abolissant les distances géographiques ou en facilitant les passages entre entreprises, équipes, employés et leur domicile, le numérique permet d'envisager des modes d'organisation plus souples, propices à une meilleure qualité de vie des employés. Pour le télétravail, des entreprises gagnent à intégrer en amont une prise en compte précise des contenus et conditions de réalisation du travail, pour mieux anticiper sur les conséquences en matière de management de l'activité quotidienne. Car ceci est un autre aspect bien connu, les pratiques de travail qui se développent autour des outils numériques mettent sous tension la structure pyramidale de l'entreprise. En favorisant une communication transversale entre les employés (messageries, réseaux sociaux et communautés de pratiques), cela ouvre des horizons possibles pour le travail collaboratif et l'intelligence collective. Mais ces modes de travail bousculent les groupes professionnels, déstructurent les cadres organisationnels et la qualité des relations de travail qui s'y déploient, générant des tensions autour des enjeux d'autonomie et de contrôle, d'engagement et de reconnaissance de la contribution des travailleurs. Le management est alors contraint de reconsidérer sa posture et ses pratiques. Parallèlement, les systèmes d'information démultiplient les dispositifs de reporting, augmentant ainsi la charge gestionnaire des employés et managers et renforçant le poids du contrôle. Ici encore, la stratégie managériale tient une place décisive. Le management de proximité pourrait être l'un des éléments charnières de la réussite ou de l'échec de la transformation numérique du travail. Comment permettre aux collaborateurs de redonner à leur travail une perspective globale ? Comment autoriser les managers de proximité à y contribuer en ménageant des temps de dialogue et en saisissant des opportunités de réappropriation collective des savoirs ? Pour un nombre limité d'entreprises novatrices sachant prendre appui sur les potentialités du numérique dans une logique de régulation sociale, combien d'autres peinent à reconsidérer leur manière d'organiser le travail ?

3.3.3 L'utilité des technologies dans les organisations :

L'évolution des outils numériques renvoie à la dimension d'utilité pour les organisations. Nous assisterons à une disparition progressive de nombreux postes peu qualifiés et à l'émergence de nouvelles tâches nécessitant des compétences spécifiques. Autrement dit, le numérique ne vient pas remplacer le travail, il va remodeler les contours de celui-ci, engager de nouvelles formes de coopération sur le marché de l'emploi, offrir aux employés, aux équipes au sein des organisations la possibilité de s'autoréguler, leur permettre de gagner en autonomie et en responsabilités. Les conséquences les plus importantes de l'automatisation et de la numérisation de l'industrie ne seront pas liées aux emplois détruits mais aux changements dans la nature des emplois, les robots ne remplacent pas des métiers mais des tâches. Les métiers évoluent, les besoins en compétences se modifient. Les tâches manuelles se complexifient, le travail devient plus intellectuel, plus diversifié. On retrouve dans plusieurs entreprises à dimension internationale une grande division du travail conformément au modèle bureaucratique. Cela correspond : à une représentation de l'organisation centrée sur des flux continus d'activités allant d'un prestataire vers un destinataire, client, usager ou bénéficiaire, il englobe les techniques, outils et méthodes supposés permettre de parvenir à cet objectif. Ce modèle d'organisation ne concerne pas que le secteur tertiaire, aujourd'hui les entreprises démontrent des tendances à l'isomorphisme mimétique. Elles recherchent à modéliser des fonctionnements, permettant de passer de l'input à l'output. L'objectif étant de modéliser numériquement des processus collaboratifs, des process humains et que ces systèmes d'informations aient la capacité d'articuler les activités collectives des employés. Si la mise en place d'outils numériques au sein des entreprises est considérée comme le moyen de répondre à la concurrence, aux enjeux commerciaux, aux enjeux de rentabilité, remplacer des tâches répétitives sans valeur ajoutée par une application numérique permet aux employés de libérer leur temps sur des sujets où le numérique ne peut pas encore intervenir (l'outil n'étant pas paramétré pour des situations incertaines et complexes). Le numérique permet également de déplacer l'utilisation sur le client en le responsabilisant et en le rendant autonome. L'entreprise se libère ainsi de certaines contraintes assez subtilement en surfant sur la tendance qu'ont les consommateurs aujourd'hui à rechercher seuls des informations, à participer et à construire leur produit, leur achat. En interne, le risque pour une organisation étant de déployer une multitude de progiciels de gestion intégrés demandant aux employés de naviguer entre plusieurs interfaces. Les employés dans le cadre de leur travail font preuve de régulation autonome face à l'augmentation des formalisations, des procédures à suivre, des process, des outils à utiliser, face de fait aux différentes injonctions paradoxales que peuvent produire l'utilisation de

plusieurs outils numériques. Ce qui revient pour un individu à choisir parfois le visible à l'invisible, traiter inconsciemment une tâche répondant aux besoins de son organisation et ainsi pour obtenir une reconnaissance de sa hiérarchie, sélectionner le travail nourrissant certains indicateurs (prenant différentes formes telles que les ratios, statistiques, tableaux de bord). Certains indicateurs auront plus d'impacts et de poids dans la vie d'une organisation que d'autres. Il s'agit des indicateurs prégnants. Ces derniers ont une symbolique particulière de par leur visibilité. Cette visibilité impacte les attitudes et les comportements des individus en situation de travail ; ils tendent à normer, à exprimer une règle à suivre, apportent une tendance de la performance de l'entreprise, ils modélisent et quantifient un évènement. La question que l'on peut se poser est de savoir si représenter une organisation par un ou des indicateurs n'est pas réducteur ? et d'ajouter à cela que sans interprétation par un individu, ils ne peuvent capturer réellement une réalité. Pour que ces indicateurs prégnants puissent mobiliser les individus autour d'un objectif commun, ils doivent être portés par des acteurs légitimes au sein de l'organisation.

3.3.4 Les effets du numérique sur les conditions de travail :

Les conditions de travail sont-elles impactées par l'utilisation des TIC ? Pas si simple de répondre à cette question. La réponse varie selon que l'utilisateur est mobile ou sédentaire, connecté ou non à un réseau et a un usage peu intensif, modéré ou intensif.

Impact positif : l'usage des TIC peut entrainer un développement de l'autonomie au travail, un sentiment de satisfaction ou une relation de confiance entre l'entreprise et l'employé. Des éléments pris en compte dans la qualité de vie au travail…

Impact négatif : les TIC peuvent, inversement, être associées à des conditions de travail dégradées et des facteurs de risques psychosociaux.

Par exemple, en cas de travail mobile et d'usage des TIC, la charge de travail et la charge mentale sont dites importantes et les employés évoquent un débordement du travail sur la sphère privée.

Les utilisateurs d'outils numériques connectés mais sédentaires déclarent avoir une charge de travail importante malgré des postes a priori plutôt routiniers et une pénibilité physique moindre. Bien qu'ils disposent de marges de manœuvre relativement importantes, ces employés ne bénéficient pas d'autant de reconnaissance que les utilisateurs d'outils mobiles.

Catégorie moins visible, les employés équipés d'outils informatiques mais ne disposant pas de messagerie électronique ni d'accès à Internet cumulent contraintes physiques et travail intense, faibles marges de manœuvre et soutien social faible. Face à un travail prescrit et

normé, et malgré des cadences élevées, leur sentiment de pression au travail ou de charge de travail excessive est néanmoins plus faible que celui du reste des utilisateurs d'outils informatiques.
Le débat n'est donc pas terminé sur les liens entre TIC et conditions de travail…

3.4 L'identité Numérique en entreprise

3.4.1 Définition et importance

À de nombreux égards, l'identité numérique est une force pour l'entreprise : elle témoigne d'une image de marque bien établie et d'un nom reconnaissable, qu'il s'agisse de vendre des produits/services ou d'échanger des documents. Mais, faute d'être maîtrisée, cette identité immatérielle peut rapidement se transformer en faiblesse, et fragiliser ce que l'organisation a mis pendant des années pour forger le socle de confiance sur lequel repose sa pérennité (Vol de données, modification ou altération de documents, pillage d'informations sensibles ou de secrets de fabrication, manipulation ou usurpation d'identité). Les risques que fait peser la numérisation de l'identité sur l'entreprise sont nombreux et doivent être pris au sérieux. Le concept d'identité s'est imposé et est devenu courant, car sans identité notre société ne peut reconnaître l'existence de droits comme la propriété, l'accès à des services administratifs, sociaux, financiers, ou constater la bonne exécution de devoirs. Prouver son identité numérique est rendu encore plus nécessaire par la multiplication des transactions électroniques, qui par essence sont effectuées à distance et non en face à face. Du fait des moyens et bénéfices qu'elle apporte, l'identité est devenue l'objet de fraudes. Vous procédez à un achat en ligne. Pour payer, vous pouvez opter pour le paiement par carte bancaire, en communiquant les informations N° de carte, date de validité et le code de sécurité. Toutes ces informations sont marquées en clair sur la carte. Toute personne qui a eu la carte entre ses mains, ne serait-ce que quelques instants, peut en prendre connaissance, et donc s'en servir frauduleusement.

À cela, il faut ajouter une autre dimension liée à la dématérialisation des échanges : l'identité numérique désigne l'identité assumée, en ligne, par l'émetteur d'un document ou d'un ordre de décision. Cela fonctionne de la même manière pour les personnes physiques et morales. Par exemple, un DRH qui signe un contrat d'embauche et l'envoie par email à la personne recrutée utilise son identique numérique – à ceci près que, dans une entreprise, chaque collaborateur est garant de l'intégrité de l'identité de l'ensemble de la structure.

3.4.2 Les différentes couches de l'identité Numérique

L'identité numérique est constituée d'une succession de trois couches informatives :

- La 1ère couche est **l'identité déclarative**. Elle englobe les données qui sont partagées par l'entreprise sur les réseaux, de façon volontaire : sur ses supports web (site internet, blog, profils sociaux), sur des supports tiers (sites d'actualités, annuaires professionnels, forums, sites informatifs…), via des photos ou des vidéos, etc. Tous les collaborateurs de l'entreprise participent à la constitution de l'identité numérique déclarative, directement ou indirectement (par exemple, en indiquant sur leur profil LinkedIn qu'ils travaillent pour telle société).
- La 2e couche est **l'identité agissante**. Elle regroupe toutes les traces laissées par les individus sur les réseaux, à l'exemple de la géolocalisation, des habitudes de navigation sur Internet (via les cookies), des échanges personnels et professionnels (par mail, via une messagerie instantanée, etc.), ou des ressources consultées sur le web (musique, vidéo, etc.). Cette facette de l'identité numérique est uniquement le fait des personnes physiques, mais l'empreinte digitale ainsi laissée peut impacter la notoriété de l'entreprise.
- La 3e couche est **l'identité calculée**. Elle est forgée par des algorithmes qui interprètent les données collectées pour recomposer les différentes facettes d'une identité individuelle ou collective. Ces outils extrapolent dans le but de prévoir les besoins et d'y répondre de façon anticipée.

Là encore, il est possible d'ajouter une pierre à l'édifice et de compléter le mille-feuille avec une 4e couche : **l'identité légale**. Elle désigne à la fois l'identité dématérialisée d'un individu ou d'une entreprise (nom et prénom, ou dénomination sociale) et les outils utilisées pour la justifier légalement (certificat électronique, signature électronique, authentification forte, etc.). Ces outils d'identité numérique n'ont pas d'autre but que de permettre les processus :

• d'identification : présenter une identité

• d'authentification : vérifier l'identité revendiquée par une personne, au moyen d'un objet qu'il possède, d'une information qu'il connaît, ou encore par une des caractéristiques physiques personnelles (biométrie). On parle d'authentification forte lorsque deux moyens sont mis en œuvre, par exemple un objet possédé plus la connaissance d'un secret. Par opposition, l'identification en tapant au clavier un identifiant et l'authentification en tapant un mot de passe

n'apportent pas une sécurité suffisante dès lors que des enjeux commerciaux ou de protection de données sont en cause.

• de signature électronique : comme pour la signature manuelle, il s'agit d'engager sa responsabilité (commande, signature d'un contrat, etc.), et encore mieux, la signature électronique permet en plus de protéger le contenu du document (son intégrité).

Dans une transaction, ces processus s'appliquent aux deux parties concernées. Les techniques mises en œuvre par les processus d'identification / authentification permettent de plus de créer un canal sécurisé pour le transfert d'informations (protection de la confidentialité et de l'intégrité des données communiquées).

Il ne s'agit en aucune façon de moyens visant à :

• surveiller les allées et venues des citoyens ;

• tracer les personnes dans leurs activités (qu'elles soient privées ou professionnelles) ;

• s'approprier ou centraliser des données personnelles ;

3.4.3 Les enjeux liés des identités numériques en entreprise

Les problématiques qui entourent l'identité numérique de l'entreprise ne peuvent plus être ignorées. Tous les secteurs d'activité sont touchés, ainsi que toutes les tailles d'entreprises. Ces dernières laissent des traces sur le web et sont susceptibles d'envoyer ou de recevoir des documents sensibles. Pour cette raison, elles sont concernées par les enjeux liés à l'identité digitale, qui se déploient à trois niveaux : branding, notoriété et cybersécurité.

- Le branding : L'image que l'entreprise projette d'elle-même à travers ses ressources propres (logo, site web, visuels, publicités) est dépassée par l'image bâtie par les utilisateurs (prospects, clients, partenaires, fournisseurs, concurrents, détracteurs, etc.). Résorber ou, du moins, contrôler l'écart qui existe entre ces deux images est l'un des enjeux majeurs de ce début de XXI^{e} siècle en termes de maîtrise de l'identité numérique. Le risque étant de laisser la parole aux utilisateurs et de négliger les contenus malveillants et les erreurs d'interprétation.
- La notoriété : Si la réputation a toujours été un enjeu déterminant pour les entreprises, l'essor du web a accentué son importance. Avec les réseaux sociaux, notamment, un bad

buzz est vite arrivé. Les mauvaises nouvelles se répandent comme une traînée de poudre, et la prolifération des fake news fait qu'il n'est même plus nécessaire qu'une information soit vraie pour convaincre une large audience. Internet est soumis à la puissance de la rumeur, avec, à la clé, des dégâts potentiellement irréversibles sur l'entreprise sa réputation étant le socle sur lequel est édifiée la confiance des tiers. Malheureusement, la notoriété ne dépend pas du bon vouloir des organisations, mais de la communauté de leurs défenseurs et de leurs détracteurs. Il est donc essentiel de suivre l'évolution de cette image de marque et d'être prêt à intervenir en cas de situation de crise.

- La Cybersécurité : Les risques pesant sur la sécurité des systèmes d'information ne cessent d'augmenter, mettant en danger à la fois les entreprises et leurs utilisateurs. Le nombre de cyberattaques contre les organisations a augmenté de 25 % en 2019, et les sociétés sont mal préparées à se défendre contre ces risques. Partout dans le monde, les attaques contre les grandes entreprises se multiplient. Les hackers profitent des failles de sécurité pour dérober des données personnelles ou lancer des logiciels malveillants.

Sachant qu'un vol de données, peut coûter en moyenne 3,54 millions d'euros et que son impact sur l'image de l'entreprise peut revenir plus cher à long terme. Sans même parler d'un autre problème, systématiquement sous-estimé : le vol de données des employés. Alors que l'accès d'une personne malveillante à des informations internes (adresses mail, conversations, fiches de paie, numéros de sécurité sociale etc.) peut avoir des conséquences majeures, notamment en donnant par la suite accès aux SI lui-même via les mots de passe dérobés.

3.4.4 Les solutions à adopter pour la sécurité de l'identité numérique de l'entreprise

Les enjeux liés à l'identité numérique et les risques relatifs à sa non-maîtrise contraignent les entreprises à prendre des mesures concrètes pour se protéger. On peut distinguer deux grandes familles de solutions à adopter :

- Les bonnes pratiques à faire appliquer au quotidien par les collaborateurs de l'entreprise (sous la houlette de la DSI). Garants de l'image de marque de leur employeur, les employés sont les premiers concernés par les bons gestes à adopter, à la fois pour conserver le contrôle de l'identité numérique de l'entreprise (attention portée aux publications et aux échanges, maîtrise de l'empreinte numérique, utilisation d'outils sécurisés pour se connecter aux réseaux, veille stratégique pour repérer les contenus

négatifs et malveillants) et pour garantir l'intégrité de cette identité lors des échanges (utilisation de mots de passe complexes changés régulièrement, connexions uniquement depuis des réseaux sécurisés, soin porté aux échanges de documents sensibles, etc.).

- Les solutions logicielles et applicatives à implémenter. Par exemple : les certificats SSL pour sécuriser l'accès au site web et aux serveurs, et ainsi garantir la confidentialité des données échangées entre les utilisateurs et l'entreprise. Les outils de signature électronique qui authentifient les émetteurs et confèrent une valeur légale aux documents digitalisés, en supprimant les risques d'altération de ces documents ou d'usurpation d'identité. Ou encore l'utilisation d'un mécanisme d'authentification forte, qui requiert la consécution d'au moins deux facteurs d'identification afin de renforcer la sécurité des accès aux SI de l'entreprise. Tous ces outils sont rattachés à des certificats électroniques délivrés par des tiers de confiance.

En somme, l'identité numérique de l'entreprise doit s'appuyer en simultané sur un ensemble de bonnes pratiques internes et sur l'utilisation d'outils sécurisés et 100 % fiables, adaptés au niveau de risque. C'est la seule façon que les organisations disposent pour reprendre le contrôle de leur identité digitale.

Chapitre 4 : Politique de sécurité

De nos jours les entreprises sont de plus en plus connectées tant en interne que dans le monde entier, profitant ainsi de l'évolution des réseaux informatiques et la dématérialisation des documents. De ce fait, leur système d'information est accessible de l'extérieur pour leurs fournisseurs, clients, partenaires et administrations. L'accessibilité par l'extérieur entraine la vulnérabilité vis à vis les attaques, mais aussi on peut pas négliger les menaces qui viennent de l'intérieur, ce qui rend l'investissement dans des mesures de protection et de sécurité indispensable, et la mise en œuvre d'un plan de sécurité issu d'un examen méthodique d'une situation liée à la sécurité de l'information en vue de vérifier sa conformité à des objectifs, à des règles, et à des normes ou référentiels, afin de cerner les différentes composantes de la sécurité du Système d'Information, et pour atteindre un niveau de sécurisation répondant aux objectifs organisationnels et techniques.

4.1. La Sécurité de l'Information :

4.1.1 C'est quoi la Sécurité de l'information ?

Pour des soucis d'efficacité et de rentabilité, une entreprise communique aujourd'hui avec ses filiales, ses partenaires et va jusqu'à offrir des services aux particuliers, ce qui induit une ouverture massive à l'information. Par l'ouverture des réseaux, la sécurité devient un facteur décisif du bon fonctionnement de l'entreprise ou de l'organisme. Il reste qu'une entreprise ou un organisme possède certaines informations qui ne doivent être divulguées qu'à un certain nombre de personnes ou qui ne doivent pas être modifiées ou encore qui doivent être disponibles de manière transparente à l'utilisateur. Ces informations feront l'objet d'une attaque par ce que des menaces existent et que le système abritant ces informations est vulnérable. Par conséquent on appelle sécurité de l'information, l'ensemble des moyens techniques, organisationnels, juridiques, et humains mis en place pour faire face aux risques identifiés, afin d'assurer la confidentialité, l'intégrité, la disponibilité, et la Traçabilité de l'information traitée :

- La Confidentialité : l'information ne doit pas être divulguée à toute personne, entité ou processus non autorisé. En clair, cela signifie que l'information n'est consultable que par ceux qui ont le droit d'y accéder.
- L'Intégrité : le caractère correct et complet des actifs doit être préservé. En clair, cela signifie que l'information ne peut être modifiée que par ceux qui en ont le droit.
- La Disponibilité : l'information doit être rendue accessible et utilisable sur demande par une entité autorisée. Cela veut dire que l'information doit être disponible dans des conditions convenues à l'avance.
- La Traçabilité (ou « Preuve ») : garantie que les accès et tentatives d'accès aux éléments considérés sont tracés et que ces traces sont conservées et exploitables.

4.2 Les risques informatiques :

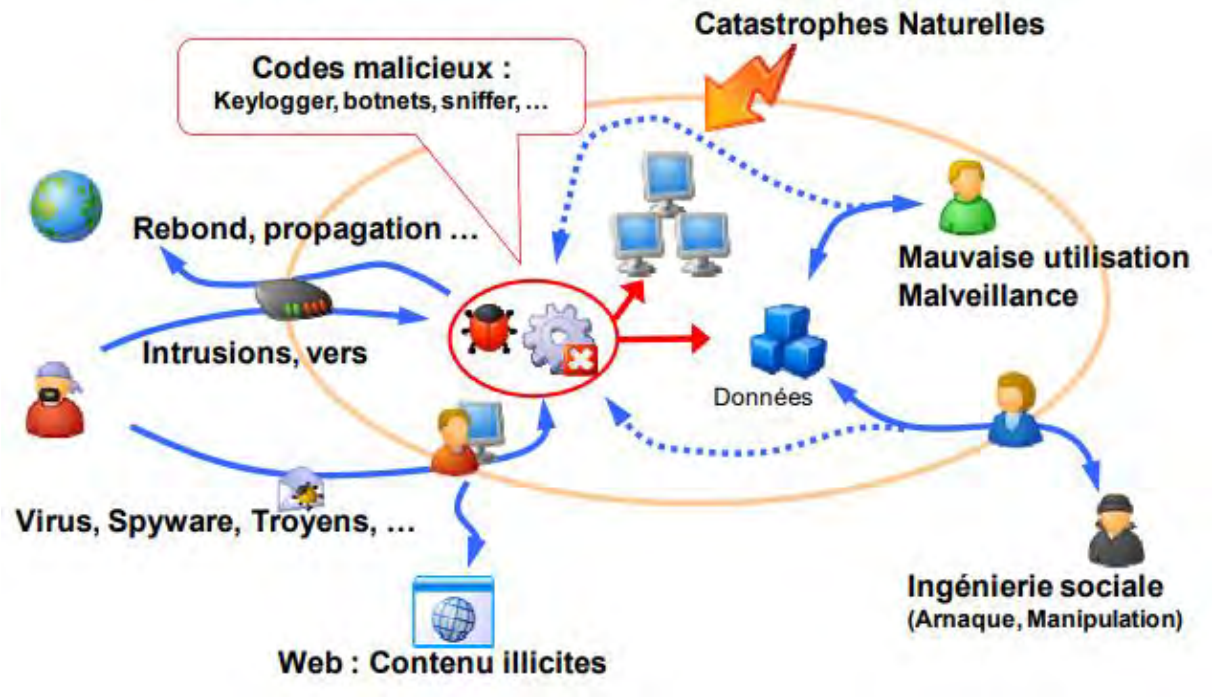

Figure 6 : les attaques informatiques

4.2.1 Généralités :

Les développements ci-dessous décrivent, pour chaque risque informatique, les principaux facteurs de risque et les contrôles ou procédures qui doivent être mis en place pour prévenir, réduire voire supprimer ce risque. Pour mémoire, l'externalisation d'un service SI conduit à transférer les risques, sans pour autant les couvrir de manière certaine. En matière informatique, comme dans tous les autres domaines, l'externalisation d'un risque ne dispense ainsi pas une organisation de s'assurer qu'il est effectivement maîtrisé par son cocontractant et ne l'exonère en rien de sa responsabilité finale.

Les principaux risques informatiques peuvent être regroupés en 3 domaines :

- les risques opérationnels, qui sont les plus nombreux pour le sujet traité ;
- les risques financiers, puisque l'informatique et l'information sont des actifs ;
- les risques légaux de non-conformité, puisque les entités sont soumises à des normes internes et externes, certaines de portée légale, concernant la gestion du SI.

4.2.2 LES PRINCIPAUX RISQUES INFORMATIQUES

Les principaux risques, facteurs de risques et dispositifs ou moyens de contrôles des risques informatiques sont les suivants :

- **Inadéquation du SI avec la stratégie de l'entité et les besoins des utilisateurs**

- Facteurs de risque :
  - Manque d'implication de la direction dans la gestion de l'informatique ;
  - Absence de schéma directeur ;
  - Absence de gouvernance informatique ;
  - Manque d'implication des utilisateurs dans les projets informatiques ;
  - Absence d'analyse de la valeur des SI mis en place.
- Contrôles ou procédures attendus :
  - Supervision de l'informatique par la direction de l'entité ;
  - Existence d'une stratégie en adéquation avec la stratégie de l'organisation, traduite par exemple dans un schéma directeur informatique ;
  - Gouvernance informatique en place et validée par la direction ;
  - Analyse de la valeur (par exemple par MAREVA 2) ;
  - Forte implication des utilisateurs (« bureaux métiers ») dans les projets informatiques.

Incapacité de l'organisation à redémarrer les systèmes informatiques en cas arrêt ou destruction

- Facteurs de risque :
  - Absence de sauvegarde régulière du SI (sauvegardes externes) ;
  - Absence de plan de secours ;
  - Absence de site de secours.
- Contrôles ou procédures attendus :
  - Mise en place d'un plan de secours (documenté, mis à jour lors de modifications majeures de l'environnement informatique, et testé au moins une fois par an) ;
  - Procédure de sauvegarde quotidienne des données et programmes critiques ;
  - Stockage des sauvegardes à l'extérieur de l'entité ;
  - Les sauvegardes doivent être testées régulièrement ;
  - Lorsqu'une activité est fortement dépendante de l'informatique, mise en place d'un site de secours.

Sécurité du SI inadaptée au niveau de risque identifié et accepté par la direction

- Les facteurs de risque sont multiples car la sécurité est transversale à tous les processus de l'informatique :
  - Sécurité physique ;
  - Sécurité logique ;

  - Sécurité du réseau ;
  - Sécurité de l'exploitation ;
  - Sécurité des PC ;
  - Sécurité des données ;
- Contrôles ou procédures attendus :
  - Politique de sécurité en place, validée et supportée par la direction de l'entité ;
  - Outils de surveillance du système informatique (par exemple supervision) ;
  - Équipe sécurité dédiée recensant tous les incidents relatifs à la sécurité et capable d'intervenir en cas d'événement de sécurité.

Accès aux données et aux applications par des personnes non autorisées

- Facteurs de risque :
  - Absence de politique de sécurité ;
  - Absence de gestion rigoureuse d'attribution des droits d'accès ;
  - Absence de gestion rigoureuse des points d'accès ;
  - Systèmes informatiques ne permettant pas une gestion fine des droits d'accès ;
  - Gestion des mots de passe insuffisante.
- Contrôles ou procédures attendus :
  - Politique de sécurité validée par la direction de l'entité ;
  - Politique de gestion des mots de passe efficace ;
  - Gestion rigoureuse des droits d'accès au système d'information en cohérence avec la séparation fonctionnelle des tâches ;
  - Revue régulière de la liste des habilitations, application par application ;
  - Revue régulière des points d'accès ;
  - Séparation des tâches effective entre les fonctions développements et exploitation ;
  - Supervision des profils sensibles alloués au personnel informatique ;
  - Traçabilité des accès et actions sensibles.

Applications informatiques non fiables

- Facteurs de risque :
  - Erreurs dans la programmation des applications par rapport aux spécifications fonctionnelles ;
  - Applications insuffisamment testées ;
  - Utilisateurs insuffisamment impliqués dans les phases de développements de l'application.

- Contrôles ou procédures attendus :
  - Forte implication des utilisateurs dans les développements informatiques ;
  - Bonne gestion de projet ;
  - Veille environnementale ;
  - Procédures de recensement des anomalies ;
  - Procédures de maintenances correctives, adaptatives et évolutives.

Indisponibilité du système informatique

- Facteurs de risque :
  - Mauvaise gestion de l'environnement matériel du SI (énergie, climatisation, protection physique, etc.) ;
  - Absence de convention de service ;
  - Absence d'outil de surveillance de la disponibilité du SI ;
  - Absence de cellule réactive en cas d'indisponibilité ;
  - Absence de contrat de maintenance des matériels informatiques.
- Contrôles ou procédures attendus :
  - Convention de service entre l'informatique et les utilisateurs, portant notamment sur des objectifs de performance du SI, tels le niveau de disponibilité des serveurs ;
  - Support utilisateur performant ;
  - Procédure de gestion des anomalies ;
  - Procédure de maintenance corrective des applications informatiques ;
  - Contrats de maintenance des matériels informatiques ;
  - Environnement matériel adapté ;
  - Plans de continuité et de reprise de l'activité.

Mauvaise utilisation du SI par les utilisateurs

- Facteurs de risque :
  - Applications informatiques non conviviales ;
  - Utilisateurs insuffisamment formés ;
  - Documentation utilisateur insuffisante et pas mise à jour ;
  - Manque de contrôles bloquants dans les applications informatiques.
- Contrôles ou procédures attendus :
  - Applications faciles d'utilisation ;
  - Formation initiale des utilisateurs réalisée en temps utile et complétée par une formation au fil de l'eau ;

- Documentation utilisateur complète et mise à jour régulièrement ;
- Contrôles bloquants dans les applications ;

  Procédures de gestion des maintenances évolutives, adaptatives et correctives.

SI non conforme avec la législation

- Les lois et décrets portant sur le renforcement des procédures de contrôles internes concernent pour partie l'informatique. Les actions à mettre en place font, pour la plupart, partie des recommandations déjà citées pour couvrir certains risques informatiques comme :
- La politique de sécurité informatique ;
- La documentation informatique à jour ;
- La sécurité des développements informatiques ;
- La gestion rigoureuse des droits d'accès au SI.
- S'agissant des déclarations CNIL, il est recommandé qu'une personne soit spécifiquement désignée dans l'organisation pour gérer ce sujet et l'anticiper. Elle doit notamment sensibiliser sur le sujet les services en charge des développements informatiques.

SI non pérenne

- Facteurs de risque :
  - Utilisation de la sous-traitance informatique sans transfert de compétence en interne ;
  - Documentation informatique inexistante ou non mise à jour suite aux évolutions du SI ;
  - Obsolescence de l'application ou de la technologie utilisée ;
  - Forte dépendance vis-à-vis de personnes clés qui peuvent quitter l'entité.
- Contrôles ou procédures attendus :
  - Le SI doit faire l'objet d'un schéma directeur informatique ;
  - La documentation informatique doit être complète et à jour, notamment dans un contexte de forte utilisation de la sous-traitance ou d'applications anciennes ;
  - Des procédures de transfert de compétence entre les sous-traitants et les équipes informatiques internes doivent être mises en place.

Les progiciels de gestion intégrés (PGI) constituent un cas particulier, porteurs d'avantages, d'inconvénients et de risques spécifiques. Les PGI présentent l'avantage de couvrir plusieurs domaines métiers d'une entreprise en une seule application par l'intermédiaire de modules. Les risques liés aux PGI sont les suivants :

• dérapage des projets (dans le temps et dans les coûts) compte tenu de la complexité et des enjeux ;

• les développements de programmes spécifiques éloignent l'outil du standard ce qui entraîne des problèmes de maîtrise du PGI voire des problèmes en termes d'audibilité ;

• une inadaptation du PGI à l'organisation dans le cas où la refonte des processus n'a pas été préalablement conduite et portée par la direction générale ;

• utilisateurs insuffisamment formés qui rejettent l'application ;

• forte dépendance vis-à-vis du sous-traitant et insuffisance de transfert de compétence en interne sur le PGI ;

• paramétrage des droits d'accès et des profils utilisateurs souvent galvaudé lors de la phase de développement.

Conformément aux pratiques de l'audit, ces risques sont habituellement analysés à travers une matrice des risques spécifiques.

4.2.3Gestion d'un réseau sécurisé :

L'atténuation des attaques réseau nécessite une approche globale de bout en bout qui inclut la création et le maintien de politiques de sécurité basées sur les besoins de sécurité d'une organisation. La première étape dans l'établissement des besoins de sécurité d'une organisation consiste à identifier les menaces probables et à effectuer une analyse des risques.

L'analyse des risques est l'étude systématique des incertitudes et des risques. Il estime la probabilité et la gravité des menaces pesant sur un système et fournit à une organisation une liste de priorités. Les analystes des risques identifient les risques ; déterminer comment et quand ces risques pourraient survenir, et estimer l'impact financier et commercial des résultats défavorables. Les résultats de l'analyse des risques sont utilisés pour déterminer les implémentations matérielles et logicielles de sécurité, les politiques d'atténuation et la conception du réseau.

L'architecture de sécurité est une solution complète pour la sécurité du réseau qui comprend des solutions pour sécuriser le réseau, la messagerie électronique, le Web, l'accès, les utilisateurs mobiles et les ressources du centre de données. Pour simplifier la conception du réseau, il est recommandé que tous les mécanismes de sécurité proviennent d'un seul fournisseur.

Une fois le réseau conçu, la sécurité des opérations implique les pratiques quotidiennes nécessaires pour d'abord déployer puis maintenir le système sécurisé. Les tests de sécurité

du réseau font partie du maintien d'un système sécurisé. Les tests de sécurité sont effectués par l'équipe des opérations, pour s'assurer que toutes les implémentations de sécurité fonctionnent comme prévu. Les tests sont également utilisés pour fournir un aperçu de la planification de la continuité des activités, qui traite des opérations continues d'une organisation en cas de catastrophe, de perturbation ou d'interruption de service prolongée.

Après la mise en œuvre d'un réseau sécurisé et l'établissement de plans de continuité, ces plans et documents doivent être continuellement mis à jour en fonction des besoins changeants de l'organisation.

La figure montre un collage des extrémités de câble RJ45 branchées et du code de programmation.

4.2.3.1. Sécurité des Opérations

La sécurité des opérations concerne les pratiques quotidiennes nécessaires pour d'abord déployer puis maintenir un système sécurisé. Tous les réseaux sont vulnérables aux attaques si la planification, la mise en œuvre, les opérations et la maintenance du réseau ne respectent pas les pratiques de sécurité opérationnelle.

La sécurité des opérations commence par le processus de planification et de mise en œuvre d'un réseau. Au cours de ces phases, l'équipe des opérations analyse les conceptions, identifie les risques et les vulnérabilités et procède aux adaptations nécessaires. Les tâches opérationnelles réelles commencent après la mise en place du réseau et incluent la maintenance continue de l'environnement. Ces activités permettent à l'environnement, aux systèmes et aux applications de continuer à fonctionner correctement et en toute sécurité.

Certaines techniques de test de sécurité sont principalement manuelles, tandis que d'autres sont hautement automatisées. Quel que soit le type de test, le personnel qui met en place et effectue les tests de sécurité doit avoir des connaissances importantes en matière de sécurité et de mise en réseau dans ces domaines :

- Durcissement de l'appareil
- Pare-feu
- IPS
- Systèmes d'exploitation
- Programmation de base
- Protocoles de mise en réseau, tels que TCP / IP
- Vulnérabilités du réseau et atténuation des risques

4.2.3.2 Test et évaluation de la sécurité du réseau

L'efficacité d'une solution de sécurité des opérations peut être testée sans attendre qu'une menace réelle se produise. Les tests de sécurité du réseau rendent cela possible. Les tests de sécurité du réseau sont effectués sur un réseau pour garantir que toutes les implémentations de sécurité fonctionnent comme prévu. En règle générale, les tests de sécurité du réseau sont effectués pendant les étapes de mise en œuvre et d'exploitation, après que le système a été développé, installé et intégré.

Les tests de sécurité fournissent un aperçu de diverses tâches administratives, telles que l'analyse des risques et la planification d'urgence. Il est important de documenter les résultats des tests de sécurité et de les mettre à la disposition du personnel impliqué dans d'autres domaines informatiques.

Au cours de la phase de mise en œuvre, des tests de sécurité sont effectués sur des parties spécifiques du réseau. Une fois qu'un réseau est entièrement intégré et opérationnel, un test et une évaluation de sécurité (ST&E) sont effectués. Un ST&E est un examen des mesures de protection placées sur un réseau opérationnel. La figure décrit les objectifs de ST&E.

Les tests doivent être répétés périodiquement et chaque fois qu'une modification est apportée au système. Pour les systèmes de sécurité qui protègent les informations critiques ou protègent les hôtes exposés à une menace constante, les tests de sécurité doivent être effectués plus fréquemment.

4.2.3.3 Types de Tests de réseau

Une fois qu'un réseau est opérationnel, vérifiez son état de sécurité. De nombreux tests de sécurité peuvent être effectués pour évaluer l'état opérationnel du réseau :

- Test de pénétration : Les tests de pénétration du réseau, ou test du stylet, simulent des attaques provenant de sources malveillantes. Le but est de déterminer la faisabilité d'une attaque et les conséquences possibles si elle devait se produire.
- Analyse réseau : Inclut un logiciel qui peut envoyer une requête ping aux ordinateurs, rechercher les ports TCP d'écoute et afficher les types de ressources disponibles sur le réseau. Certains logiciels de numérisation peuvent également détecter les noms d'utilisateur, les groupes et les ressources partagées. Les administrateurs réseau peuvent utiliser ces informations pour renforcer leurs réseaux.
- Analyse des vulnérabilités : Inclut un logiciel capable de détecter les faiblesses potentielles des systèmes testés. Ces faiblesses peuvent inclure une mauvaise configuration, des mots de passe vides ou par défaut, ou des cibles potentielles d'attaques

DoS. Certains logiciels permettent aux administrateurs de tenter de planter le système via la vulnérabilité identifiée.

- Cracking de mot de passe **:** Inclut un logiciel utilisé pour tester et détecter les mots de passe faibles qui doivent être modifiés. Les politiques de mot de passe doivent inclure des directives pour éviter les mots de passe faibles.
- Examen des journaux : Les administrateurs système doivent examiner les journaux de sécurité pour identifier les menaces de sécurité potentielles. Une activité anormale doit être étudiée à l'aide d'un logiciel de filtrage pour analyser de longs fichiers journaux.
- Vérificateurs d'intégrité **-** Un système de vérification d'intégrité détecte et signale les changements dans le système. La plupart des contrôles sont concentrés sur le système de fichiers. Cependant, certains systèmes de vérification peuvent rendre compte des activités de connexion et de déconnexion.
- Détection de virus : Un logiciel de détection de virus peut être utilisé pour identifier et supprimer les virus informatiques et autres logiciels malveillants.

4.2.3.4 Application des résultats des tests de réseau :

Les résultats des tests de sécurité réseau peuvent être utilisés de plusieurs manières :

- Pour définir les activités d'atténuation pour traiter les vulnérabilités identifiées
- Comme référence pour suivre les progrès d'une organisation dans la satisfaction des exigences de sécurité
- Pour évaluer l'état de mise en œuvre des exigences de sécurité du système
- Effectuer une analyse des coûts et des avantages pour améliorer la sécurité du réseau
- Améliorer d'autres activités, telles que l'évaluation des risques, la certification et l'autorisation (C&A), et les efforts d'amélioration des performances
- Comme point de référence pour l'action corrective

4.2.3.4.1 Outils de test de réseau :

Il existe de nombreux outils disponibles pour tester la sécurité des systèmes et des réseaux. Certains de ces outils sont open source tandis que d'autres sont des outils commerciaux qui nécessitent une licence. Divers outils logiciels peuvent être utilisés pour effectuer des tests de réseau, notamment :

- Nmap / Zenmap : Découvre des ordinateurs et des services sur un réseau informatique, créant ainsi une carte du réseau

- SuperScan : Logiciel d'analyse de port conçu pour détecter les ports TCP et UDP ouverts, déterminer les services exécutés sur ces ports et exécuter des requêtes, telles que whois, ping, traceroute et recherches de nom d'hôte
- SIEM (Security Information Event Management) : Une technologie utilisée dans les organisations d'entreprise pour fournir des rapports en temps réel et une analyse à long terme des événements de sécurité
- GFI LANguard : Scanner de réseau et de sécurité qui détecte les vulnérabilités

- Tripwire : Évalue et valide les configurations informatiques par rapport aux politiques internes, aux normes de conformité et aux meilleures pratiques de sécurité

- Nessus : Logiciel d'analyse des vulnérabilités, axé sur l'accès à distance, les erreurs de configuration et le DoS par rapport à la pile TCP / IP
- L0phtCrack : Application d'audit et de récupération de mot de passe
- Metasploit : Fournit des informations sur les vulnérabilités et facilite les tests de pénétration et le développement de signatures IDS

4.2.3.4.2 Nmap et Zenmap :

Nmap est un scanner de bas niveau couramment utilisé et accessible au public. Il possède une gamme d'excellentes fonctionnalités qui peuvent être utilisées pour la cartographie et la reconnaissance du réseau. La fonctionnalité de base de Nmap permet à l'utilisateur d'accomplir plusieurs tâches :

- Analyse classique des ports TCP et UDP : Recherche différents services sur un hôte.
- Balayage de port TCP et UDP classiques : Recherche le même service sur plusieurs hôtes.
- Analyses et balayages de ports TCP et UDP furtifs - Semblables aux analyses et balayages classiques, mais plus difficiles à détecter par l'hôte cible ou IPS.
- Identification du système d'exploitation à distance : Ceci est également connu sous le nom d'empreintes digitales du système d'exploitation.

Les fonctionnalités avancées de Nmap incluent l'analyse de protocole, connue sous le nom d'analyse de port de couche 3. Cette fonction identifie la prise en charge du protocole de couche 3 sur un hôte. Les exemples de protocoles qui peuvent être identifiés incluent GRE et OSPF.
Bien que Nmap puisse être utilisé pour des tests de sécurité, il peut également être utilisé à des fins malveillantes. Nmap a une fonctionnalité supplémentaire qui lui permet d'utiliser des hôtes leurres sur le même LAN que l'hôte cible, pour masquer la source de l'analyse.

Nmap n'a pas de fonctionnalités de couche application et fonctionne sous UNIX, Linux, Windows et OS X.

4.2.3.4.3. SuperScan :

SuperScan est un outil d'analyse de port Microsoft Windows. Il fonctionne sur la plupart des versions de Windows et nécessite des privilèges d'administrateur. SuperScan version 4 possède un certain nombre de fonctionnaliés utiles :

- Vitesse de numérisation réglable
- Prise en charge de plages IP illimitées
- Détection d'hôte améliorée à l'aide de plusieurs méthodes ICMP
- Analyse TCP SYN
- Analyse UDP (deux méthodes)
- Génération de rapport HTML simple
- Source port scanning
- Résolution rapide du nom d'hôte
- Capacités étendues de saisie de bannière
- Base de données de description de liste de ports intégrée massive
- Aléatoire d'ordre de scan IP et de port
- Une sélection d'outils utiles, tels que ping, traceroute et whois
- Capacité étendue d'énumération des hôtes Windows

4.2.3.4.4. SIEM

La gestion des événements de sécurité (SIEM) est une technologie utilisée dans les entreprises pour fournir des rapports en temps réel et une analyse à long terme des événements de sécurité. SIEM a évolué à partir de deux produits auparavant distincts : la gestion des informations de sécurité (SIM) et la gestion des événements de sécurité (SEM). SIEM peut être implémenté en tant que logiciel, intégré à Cisco Identity Services Engine (ISE) ou en tant que service géré.

SIEM combine les fonctions essentielles de SIM et SEM pour fournir :

- **Analyse judiciaire** - La possibilité de rechercher des journaux et des enregistrements d'événements à partir de sources dans toute l'organisation fournit des informations plus complètes pour l'analyse judiciaire.
- **Corrélation** - Examine les journaux et les événements de systèmes ou d'applications disparates, accélérant la détection et la réaction aux menaces de sécurité.

- **Agrégation** - L'agrégation réduit le volume de données d'événements en consolidant les enregistrements d'événements en double.
- **Rétention** - Le reporting présente les données d'événements corrélées et agrégées dans une surveillance en temps réel et des résumés à long terme.

SIEM fournit des détails sur la source de l'activité suspecte, notamment :

- Informations utilisateur (nom, état d'authentification, emplacement, groupe d'autorisation, état de quarantaine)
- Informations sur l'appareil (fabricant, modèle, version du système d'exploitation, adresse MAC, méthode de connexion réseau, emplacement)
- Informations sur la posture (conformité de l'appareil à la politique de sécurité de l'entreprise, version antivirus, correctifs du système d'exploitation, conformité à la politique de gestion des appareils mobiles)

En utilisant ces informations, les ingénieurs en sécurité réseau peuvent évaluer rapidement et précisément l'importance de tout événement de sécurité et répondre aux questions critiques :

- Qui est associé à cet événement ?
- S'agit-il d'un utilisateur important ayant accès à la propriété intellectuelle ou à des informations sensibles ?
- L'utilisateur est-il autorisé à accéder à cette ressource ?
- L'utilisateur a-t-il accès à d'autres ressources sensibles ?
- Quel type d'appareil est utilisé ?
- Cet événement représente-t-il un problème de conformité potentiel ?

4.2.3.5 Cycle de vie d'un réseau sécurisé :

Le cycle de vie du réseau sécurisé est un processus d'évaluation et de réévaluation des besoins en équipements et en sécurité à mesure que le réseau évolue. Un aspect important de cette évaluation continue est de comprendre quels actifs une organisation doit protéger, même si ces actifs évoluent.

Déterminez quels sont les atouts d'une organisation en posant des questions :

- Qu'est-ce que l'organisation a que les autres veulent ?
- Quels processus, données ou systèmes d'information sont essentiels pour l'organisation ?
- Qu'est-ce qui empêcherait l'organisation de faire des affaires ou de remplir sa mission ?

Les réponses peuvent identifier des actifs tels que des bases de données critiques, des applications vitales, des informations importantes sur les clients et les employés, des

informations commerciales classifiées, des lecteurs partagés, des serveurs de messagerie et des serveurs Web.

Les systèmes de sécurité réseau aident à protéger ces actifs, mais un système de sécurité à lui seul ne peut pas empêcher les actifs d'être vulnérables aux menaces. Les systèmes de sécurité techniques, administratifs et physiques peuvent tous être vaincus si la communauté des utilisateurs finaux ne respecte pas les politiques et procédures de sécurité.

4.2.4 LES FACTEURS CLEFS D'UN SI PERFORMANT

Un SI idéal :

• est en adéquation avec la stratégie de l'organisation et les objectifs des métiers ;
• est en conformité avec les obligations légales ;
• est sécurisé ;
• est facile à utiliser ;
• est fiable ;
• est adaptatif ;
• est pérenne ;
• est disponible ;
• est efficient ;
• respecte le plan d'urbanisme ;
• quand il fait l'objet de marchés, est conforme aux bonnes pratiques de la commande publique.

Les principaux facteurs clefs d'un SI performant sont les suivants :

• une forte implication de la direction dans la gestion du SI. Elle doit notamment superviser la gestion du SI par la mise en place des outils de pilotage suivants :

• un schéma directeur informatique (SDI), qui définit la stratégie informatique pluriannuelle, dont la validation par la direction entérine l'adéquation entre la stratégie informatique et la stratégie de l'entité ;
• des documents d'organisation de la gouvernance du SI, mis à jour régulièrement ;
• des comités de pilotage informatiques réguliers (suivi des incidents, suivi des projets, suivi des budgets, etc.), au sein desquels la direction doit être représentée à bon niveau
• des tableaux de bord de suivi de l'informatique ;
• un portefeuille des projets SI et des analyses de la valeur des systèmes d'information
• une politique de sécurité approuvée au plus haut niveau de la direction ;

• des comités de sécurité réguliers, au sein desquels la direction doit être représentée à bon niveau ;

• une cartographie des applications et systèmes informatiques à jour, incluse dans une politique d'urbanisme informatique. Cette cartographie est fondamentale pour les auditeurs, les certificateurs ou tout autre organisme de contrôle.

• une politique de sécurité, qui doit être validée et soutenue par la direction de l'entité :

• la politique de sécurité des systèmes d'information (PSSI) constitue le principal document de référence en matière de sécurité des systèmes d'information (SSI). Elle reflète la vision stratégique de l'entité et montre l'importance qu'accorde la direction à la sécurité de son SI ;

• elle se matérialise par un document présentant, de manière ordonnée, les règles de sécurité à appliquer et à respecter dans l'organisme. Ces règles sont généralement issues d'une étude des risques SSI ;

• après validation, la PSSI doit être diffusée à l'ensemble des acteurs du SI (utilisateurs, sous-traitants, prestataires, etc.). Elle constitue alors un véritable outil de communication sur l'organisation et les responsabilités SSI, les risques SSI et les moyens disponibles pour s'en prémunir ;

• la PSSI est un document vivant qui doit évoluer afin de prendre en compte les transformations du contexte de l'organisme (changement d'organisation, de missions, etc.) et des risques (réévaluation de la menace, variation des besoins de sécurité, des contraintes et des enjeux) ;

• idéalement, il devrait exister une charte d'utilisation du système d'information, dans le but de sensibiliser les utilisateurs à la sécurité informatique, informer les utilisateurs des responsabilités qui leur incombent. Pour une meilleure efficacité, cette charte devrait être signée par tous les agents et une communication régulière sur le sujet devrait être mise en place avec le support de la direction. Cette charte contiendrait par exemple les règles de sécurité et de bon usage (protection du PC, mots de passe, confidentialité, utilisation d'Internet, de la messagerie, protection du PC, etc.), les normes relatives aux logiciels (installation, licences, etc.), une description de la traçabilité des actions sur le SI à laquelle chaque utilisateur est assujetti et les sanctions applicables en cas de non-respect des règles décrites.

• le respect de la législation en matière de système d'information :

• la législation ne peut être appréciée en termes uniquement de contrainte. La mise en conformité du SI permet de garantir de façon raisonnable un environnement de contrôle satisfaisant de son SI ;

• le respect des bonnes pratiques en matière de commande publique :

• l'achat de prestations ou de logiciels est un acte complexe, qui suppose une excellente coopération entre les opérationnels et les services acheteurs. La possibilité de recourir au « sur-mesure », plus fréquente que pour d'autres types d'achats, impose en contrepartie une rigueur particulière s'agissant des spécifications, des procédures de passation et de réception et du pilotage des assistances à la MOA ou à la MOE ;
• cette complexité rend d'autant plus important le respect du code des marchés publics et des guides de bonnes pratiques rédigés par le SAE, et ce, quelle que soit la méthode de développement utilisée. Contrairement à ce que l'on entend parfois, les dispositions encadrant la commande publique sont, en effet, adaptées au domaine informatique, y compris à la méthode agile, et leur application rigoureuse et sincère peut éviter nombre de déconvenues.
• un paramétrage correct des droits d'accès aux applications informatiques :
• les droits d'accès au SI doivent refléter les règles de séparation des tâches telles que définies dans l'organisation ;
• au niveau informatique, les développeurs ne peuvent pas avoir accès à l'environnement de production et le personnel d'exploitation ne peut pas avoir accès à l'environnement de développement. Par ailleurs, l'attribution de droits très élevés (administrateurs) doit être limitée et toute action de ces profils sensibles doit être tracée et revue régulièrement ;
• au niveau des applications informatiques, les droits d'accès attribués doivent traduire de façon informatique les rôles de chacun dans l'organisation. Chaque agent n'a accès qu'aux applications qui le concernent dans sa fonction, et à l'intérieur des applications, il existe des restrictions au niveau de chaque fonctionnalité, voire au niveau des données ;
• les droits d'accès doivent faire l'objet d'une gestion rigoureuse, par un service dédié. Ainsi, les demandes d'octroi de droit d'accès doivent être formalisées et obligatoirement validées par les chefs de service. Les déblocages en cas de perte de mot de passe doivent être organisés. Enfin, la liste des habilitations, application par application, doit être revue régulièrement, et les droits d'accès supprimés en cas de départ.
• une bonne gestion des projets de développements informatiques. La réussite d'un projet informatique nécessite des éléments suivants :
• une vision claire de l'objectif et des résultats attendus ;
• l'implication de la direction générale ;
• une définition claire des responsabilités des parties prenantes ;
• l'implication des utilisateurs ;
• la constitution d'une équipe projet dédiée dirigée par des cadres expérimentés ;
• des choix techniques pérennes ;

• une gestion rigoureuse et organisée du projet ;
• un déploiement échelonné ;
• un suivi des risques ;
• un accompagnement du changement.
• un SI intégré :
• un SI est dit intégré quand toutes les applications communiquent entre elles de façon automatique à l'aide d'interfaces. Ainsi, les informations ne sont saisies qu'une seule fois dans les systèmes et les échanges de données font l'objet de contrôles d'intégrité automatiques. L'action humaine, source potentielle d'erreurs ou de fraude, est donc très limitée.
• par ailleurs, la piste d'audit peut être entièrement informatisée.
• une démarche qualité informatique : la mise en place d'une démarche qualité pour la gestion de la production et le développement informatique permet d'améliorer les performances du système d'information, de normaliser les procédures de gestion en fonction des référentiels existants et d'améliorer les compétences des acteurs du système d'information. Il existe en la matière de nombreux référentiels, dont les principaux sont les suivants :
• CMMI (Capability Maturity Model + Intégration) pour les développements informatiques (avec plusieurs niveaux de certification de 1 à 5) ;
• ITIL (Information Technology Infrastructure Library) : plus spécifique à la gestion de la production informatique ;
• COBIT (Control Objectives for Information and related Technology) : est un référentiel en matière de gouvernance informatique ;
• ISO 27001 (auparavant la BS7799) : présente les exigences en matière de sécurité informatique ;
• le « guide des bonnes pratiques des achats de services informatiques » du service des achats de l'État (SAE) ;
• les guides et recommandations sectorielles publiés par l'ANSSI et la DISIC ;
• le cadre stratégique commun du SI de l'État et le cadre commun d'urbanisation ;
• méthode MAREVA2 (Méthode d'Analyse et de Remontée de la valeur) des projets SI.

4.3 La Politique de sécurité :

Une politique de sécurité est un ensemble d'objectifs de sécurité pour une entreprise, des règles de comportement pour les utilisateurs et les administrateurs et la configuration système requise. Ces objectifs, règles et exigences assurent collectivement la sécurité d'un réseau, des données et des systèmes informatiques d'une organisation. Tout comme un plan de continuité,

une politique de sécurité est un document en constante évolution basé sur les changements de technologie, les besoins des entreprises et des employés.

Une politique de sécurité complète accomplit plusieurs tâches :

- Cela démontre l'engagement d'une organisation envers la sécurité.
- Il définit les règles du comportement attendu.
- Il garantit la cohérence des opérations du système, de l'acquisition et de l'utilisation des logiciels et du matériel et de la maintenance.
- Il définit les conséquences juridiques des violations.
- Cela donne au personnel de sécurité le soutien de la direction.

Les politiques de sécurité sont utilisées pour informer les utilisateurs, le personnel et les responsables des exigences d'une organisation en matière de protection des actifs technologiques et informationnels. Une stratégie de sécurité spécifie également les mécanismes nécessaires pour répondre aux exigences de sécurité et fournit une base de référence à partir de laquelle acquérir, configurer et auditer les systèmes informatiques et les réseaux pour la conformité.

Une politique de sécurité peut inclure les éléments suivants :

- Politiques d'identification et d'authentification : Spécifie les personnes autorisées qui peuvent avoir accès aux ressources du réseau et décrit les procédures de vérification.
- Politiques de mot de passe : Garantit que les mots de passe répondent aux exigences minimales et sont modifiés régulièrement.
- Politiques d'utilisation acceptables : Identifie les ressources et les usages du réseau qui sont acceptables pour l'organisation. Il peut également identifier des ramifications si cette politique est violée.
- Stratégies d'accès à distance : Identifie comment les utilisateurs distants peuvent accéder à un réseau et ce qui est accessible via la connectivité à distance.
- Stratégies de maintenance du réseau : Spécifie les systèmes d'exploitation des périphériques réseau et les procédures de mise à jour des applications de l'utilisateur final.
- Stratégies de gestion des incidents : Décrit comment les incidents de sécurité sont traités.

L'un des composants de politique de sécurité les plus courants est une politique d'utilisation acceptable (AUP). Cela peut également être appelé une politique d'utilisation appropriée. Ce composant définit ce que les utilisateurs sont autorisés et non autorisés à faire sur les différents composants du système. Cela inclut le type de trafic autorisé sur le réseau. La PUA doit être aussi explicite que possible pour éviter les malentendus. Par exemple, un AUP peut répertorier des sites Web spécifiques, des groupes de discussion ou des applications gourmandes en bande

passante dont l'accès est interdit aux ordinateurs de l'entreprise ou à partir du réseau de l'entreprise.

Elle reflète la vision stratégique de l'entreprise, en matière de sécurité des systèmes d'information (SSI) et de gestion de risques SSI. Elle décrit en effet les éléments stratégiques (enjeux, référentiel, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d'information de l'organisme. Elle vise à informer la maîtrise d'ouvrage et la maîtrise d'œuvre des enjeux tout en les éclairant sur ses choix en termes de gestion des risques et à susciter la confiance des utilisateurs et partenaires envers le système d'information.

Cette définition regroupe plusieurs éléments importants :

- La PSSI a une dimension stratégique : c'est un document qui exprime les orientations de l'équipe de direction de l'organisme. Cette approche top-down permet donc de fixer les enjeux en termes de sécurité informatique et de cadrer les actions à mettre en œuvre pour amoindrir les risques identifiés. Retenez qu'au travers de la PSSI, c'est le dirigeant de l'entreprise qui s'exprime ;
- La PSSI constitue un outil de communication : que ce soient vers les équipes métier (MOA) ou vers les équipes de conception et d'élaboration (MOE) des projets informatiques sur le SI, la PSSI informe sur les choix faits par l'entreprise en termes de SSI ;
- La PSSI donne un socle commun de mesures prises face au risque pour susciter la confiance des collaborateurs et des prestataires vis-à-vis du SI. À ce titre, une PSSI favorise la création de valeur pour l'entreprise en facilitant les collaborations avec son écosystème.

On vous propose de voir les lignes macroscopiques de la méthodologie proposée ici pour construire la PSSI d'une entreprise.

La méthode proposée se décompose en 4 phases principales :

Phase 1 : Donner un cadre à la démarche

Cette étape consiste à déterminer les orientations stratégiques et le périmètre de la PSSI au regard du SI, ainsi qu'à en préciser les enjeux.

Phase 2 : Faire l'inventaire des moyens du SI

On s'intéresse ici aux biens à protéger. Au sens d'EBIOS, on considère les systèmes informatiques, les organisations et les locaux. Vous devrez répertorier le patrimoine physique et l'organisation que les règles de la PSSI vont protéger.

Phase 3 : Analyser les risques

Par une méthode reconnue (EBIOS, MEHARI), vous aurez ici à déterminer une cartographie **des risques** qui pèsent sur le SI. Cet inventaire des risques, hiérarchisés par criticité, permet de sensibiliser les acteurs du SI aux différents scénarios potentiellement dangereux. Ensuite, vous devrez choisir pour chaque risque principal identifié, la manière dont il sera traité.

Phase 4 : Choisir les mesures de sécurité

Dans cette étape, il s'agit d'associer à chaque risque cartographié, les exigences de sécurité (exprimées sous forme fonctionnelle et peu technique) qui doivent être mises en œuvre pour le réduire. Pour vous aider, vous pouvez utiliser les thèmes de la norme ISO 27002 pour guider le travail. Enfin, il vous faudra décliner ces exigences en règles de sécurité, en les attachant à un des composants de l'inventaire, et en précisant l'acteur qui en aura la responsabilité.

4.3.1 Le plan Type de la PSSI :

Il existe de nombreuses variantes possibles pour une PSSI. Ne soyez donc pas étonné de trouver plusieurs déclinaisons différentes dans la littérature. Pour autant, vous trouverez bien souvent les mêmes grandes lignes. On propose un plan type qu'on pourra **adapter** aux besoins particuliers de l'entreprise.

Il est principalement constitué de deux grands axes :

	Titre	**Objectifs**	**Contenu**
1	Cadre de la PSSI	Expliciter le rôle de la PSSI pour l'entreprise Déterminer le périmètre d'application de la PSSI	
1.1	Mot de la direction	Montrer l'implication du top management. Expliciter la démarche.	Texte montrant l'importance de la démarche de PSSI pour l'organisme (Proposé par le RSSI et validé par la direction) Prise de conscience des utilisateurs (phase 1)
1.2	Enjeux et champ d'application de la PSSI	Déterminer le champ d'application.	Objet de la PSSI ;(phase 1) Activités de l'entreprise (métier et support) à intégrer et celles à

		Décliner les composants du SI à sécuriser en priorité ainsi que les risques associés.	exclure du périmètre de la PSSI. (Phase 1) Bilan des catégories de biens à protéger (phase 2)
2	Contexte	Fixer le périmètre du SI auquel doit s'appliquer la PSSI. Expliciter les enjeux de sécurité de l'entreprise. Préciser le cadre légal à respecter Affirmer les risques identifiés	
2.1	Enjeux de sécurité	Préciser pourquoi il est important, pour les activités de l'entreprise, de prendre en compte la sécurité.	Les contraintes liées au contexte, aux obligations de la structure, à l'environnement, etc. peuvent également être mentionnées ici si elles sont susceptibles de conditionner les attentes en termes de SSI. (phase 1)
2.2	Cadre légal, réglementaire et obligations contractuelles	Identifier les principaux textes, lois et règlements qui imposent des contraintes vis-à-vis de l'usage du Si de l'entreprise.	Textes législatifs majeurs : • RGPD, CNIL, Cloud Act pour les entreprises de droit américain, loi sur le secret des communications, lois sur la cryptographie, le respect du droit d'auteur le cas échéant ; • Le règlement intérieur ou la charte intérieure ; • Les grands principes d'éthique auxquels l'entreprise souscrit ; • On y ajoute tous les documents que le RSSI jugent applicables à l'entreprise en termes de SSI. Normes particulières : • RGS de l'ANSSI

			Les obligations contractuelles de l'entreprise vis-à-vis de ses clients ou partenaires (RSE par exemple) (phase 1)
2.3	Principaux risques	Lister les principaux risques pesant sur le SI, hiérarchisés par niveau de risque, afin de définir les priorités de mise en place des mesure de sécurité.	Origine des risques : En s'appuyant sur la méthodologie, vous y listerez les origines humaines délibérées, accidentelles et non humaines. Principaux risques identifiés : Issus d'une analyse de risque et proposée sous forme tabulaire, vous devrez aborder les événements redoutés, les scénarios envisagés le cas échéant, les niveaux de gravité et de vraisemblance. Stratégie de traitement des risques : Pour chaque risque identifié, vous devrez préciser l'option de stratégie macroscopique choisi (réduction, transfert, évitement, maintien). Tout cela s'effectue en phase 3.
3	Exigences et règles de sécurité	Énoncer les exigences et mesures prises en compte pour limiter les risques	Regroupées par thématiques (au sens ISO 27002 du terme que l'on verra), les exigences de sécurité applicables au périmètre de l'entreprise et les mesures mises en oeuvre pour les amoindrir.
4	Annexes	Attacher au document des éléments particuliers	Responsable sécurité de l'entreprise Glossaire Matrice de la couverture exigences / risques

Tableau 1 : Plan Type de la PSSI

On peut comprendre entre les lignes que la rédaction d'une PSSI s'appuie aussi sur l'utilisation de normes du domaine de la sécurité de l'information : la famille des **normes 2700x**. Pour compléter la vision de la PSSI, je vous propose donc, dans le chapitre suivant d'aborder ces normes et de voir leurs liens avec la PSSI.

4.3.2 Audience de la politique de sécurité

Le public de la politique de sécurité est toute personne ayant accès au réseau. L'audience interne comprend divers membres du personnel, tels que les gestionnaires et les cadres, les départements et les unités commerciales, le personnel technique et les employés. Le public externe est également un groupe varié qui comprend des partenaires, des clients, des fournisseurs, des consultants et des entrepreneurs. Il est probable qu'un document ne réponde pas aux besoins de l'ensemble du public d'une grande organisation. L'objectif est de s'assurer que les divers documents de politique de sécurité de l'information sont cohérents avec les besoins du public visé.

Le public détermine le contenu de la politique. Par exemple, il n'est probablement pas nécessaire d'inclure une description des raisons pour lesquelles quelque chose est nécessaire dans une politique destinée au personnel technique. On peut supposer que le personnel technique sait déjà pourquoi une exigence particulière est incluse. Les gestionnaires ne seront probablement pas intéressés par les aspects techniques des raisons pour lesquelles une exigence particulière est nécessaire. Au lieu de cela, ils veulent une vue d'ensemble de haut niveau ou les principes sous-tendant l'exigence. Les employés ont souvent besoin de plus d'informations sur les raisons pour lesquelles des règles de sécurité particulières sont nécessaires. S'ils comprennent les raisons des règles, ils sont plus susceptibles de les respecter.
La figure montre le public qui détermine le contenu de la politique de sécurité, comme l'utilisateur final, le gestionnaire et l'ingénieur.

4.3.4 Hiérarchie des politiques de sécurité

La plupart des entreprises utilisent une série de documents de politique pour répondre à leurs divers besoins. Ces documents sont souvent divisés en une structure hiérarchique, comme le montre la figure :

- Politique de gouvernance : Traitement de haut niveau des consignes de sécurité importantes pour l'ensemble de l'entreprise. Les gestionnaires et le personnel technique sont le public visé. La politique en vigueur contrôle toutes les interactions liées à la sécurité entre les unités commerciales et les services de soutien de l'entreprise.
- Politique technique : Utilisée par les membres du personnel de sécurité lorsqu'ils s'acquittent des responsabilités de sécurité du système. Ces politiques sont plus détaillées que la politique en vigueur et sont spécifiques au système ou à un problème spécifique. Par exemple, les problèmes de contrôle d'accès et de sécurité physique sont décrits dans une politique technique.
- Stratégie de l'utilisateur final : Couvre tous les sujets de sécurité importants pour les utilisateurs finaux. Les utilisateurs finaux peuvent inclure des employés, des clients et tout autre utilisateur individuel du réseau.

4.3.4.1 Politique de gouvernance

La politique en vigueur décrit les objectifs de sécurité généraux de l'entreprise pour les gestionnaires et le personnel technique. Il couvre toutes les interactions liées à la sécurité entre les unités commerciales et les services de soutien de l'entreprise.

La politique de gouvernance s'aligne étroitement sur les politiques existantes de l'entreprise et est placée au même niveau d'importance que ces autres politiques. Cela inclut les politiques de ressources humaines et d'autres politiques qui mentionnent des problèmes liés à la sécurité, tels que la messagerie électronique, l'utilisation de l'ordinateur ou des sujets informatiques connexes.

Une politique de gouvernance comprend plusieurs domaines :

- Énoncé du problème abordé par la politique
- Comment la politique s'applique dans l'environnement
- Rôles et responsabilités des personnes concernées par la politique
- Actions, activités et processus autorisés (et non autorisés)
- Conséquences du non-respect

4.3.4.2 Politiques Techniques

Les politiques techniques sont des documents détaillés qui sont utilisés par le personnel technique dans l'exercice de ses responsabilités quotidiennes en matière de sécurité. Ce sont essentiellement des manuels de sécurité qui décrivent ce que fait le personnel technique, mais pas comment il s'acquitte de ses fonctions.

Les politiques techniques sont décomposées en composants techniques spécifiés, notamment :

- Politiques générales : Inclut l'AUP, la politique de demande d'accès au compte, la politique d'évaluation d'acquisition, la politique d'audit, la politique de sensibilité des informations, la politique d'évaluation des risques et la politique globale du serveur Web.
- Politique de téléphonie : Définit la politique d'utilisation des lignes téléphoniques et FAX de l'entreprise.
- Politique de messagerie et de communication : Inclut une politique de messagerie générique et une politique de messagerie transférée automatiquement.

- Stratégie d'accès à distance : Inclut une stratégie VPN et peut inclure une stratégie d'accès à distance si elle est toujours prise en charge par l'organisation.

- Stratégie réseau : Inclut une stratégie extranet, des exigences minimales pour la stratégie d'accès réseau, des normes d'accès réseau, une stratégie de sécurité de routeur et de commutateur et une stratégie de sécurité de serveur.
- Stratégie d'application : Inclut une stratégie de chiffrement acceptable, une stratégie de fournisseur de services d'application (ASP), une stratégie de codage des informations d'identification de base de données, une stratégie de communication interprocessus, une stratégie de sécurité de projet et une stratégie de protection du code source.

Il peut également inclure une politique de communication sans fil qui définit des normes pour les systèmes sans fil utilisés pour se connecter au réseau.

La figure montre deux livres noirs intitulés Politique technique.

4.3.4.3 Politiques des utilisateurs finaux

Les politiques relatives aux utilisateurs finaux couvrent toutes les règles relatives à la sécurité des informations que les utilisateurs finaux doivent connaître et respecter. Ces politiques sont généralement regroupées dans un seul document pour en faciliter l'utilisation. Les politiques relatives aux utilisateurs finaux peuvent chevaucher les politiques techniques, mais peuvent également inclure :

- Stratégie d'identité **:** Définit les règles et pratiques pour protéger le réseau de l'organisation contre les accès non autorisés. Ces pratiques contribuent à réduire le risque que les informations d'identité tombent entre de mauvaises mains.
- Politique de mot de passe : Les mots de passe sont un aspect important de la sécurité informatique. Une politique de mot de passe définit les règles que tous les utilisateurs doivent suivre lors de la création et de la sécurisation de leurs mots de passe.

- Politique antivirus : Cette politique définit les normes de protection du réseau d'une organisation contre toute menace liée aux virus, vers ou chevaux de Troie.

Plusieurs groupes cibles différents nécessitent des stratégies d'utilisateur final. Chaque groupe peut devoir accepter une politique d'utilisateur final différente. Par exemple, une politique d'utilisateur final d'employé serait probablement différente d'une politique d'utilisateur final de client.

4.3.5 Documents de Politiques de sécurité

Les documents de politique de sécurité sont des documents de synthèse de haut niveau. Le personnel de sécurité utilise des documents détaillés pour mettre en œuvre les politiques de sécurité. Ceux-ci comprennent les documents sur les normes, les lignes directrices et les procédures.

Les normes, directives et procédures contiennent les détails réels définis dans les politiques. Chaque document remplit une fonction différente, couvre des spécifications différentes et cible un public différent. La séparation de ces documents facilite leur mise à jour et leur maintenance.

4.3.6 Les normes de Sécurité :

Les normes aident un personnel informatique à maintenir la cohérence dans les opérations du réseau. Les documents de normes comprennent les technologies requises pour des utilisations spécifiques, les exigences de gestion des versions du matériel et des logiciels, les exigences du programme et tout autre critère organisationnel à suivre. Cela aide le personnel informatique à améliorer l'efficacité et la simplicité dans la conception, la maintenance et le dépannage.

L'un des principes de sécurité les plus importants est la cohérence. Pour cette raison, il est nécessaire que les organisations établissent des normes. Chaque organisation élabore des normes pour soutenir son environnement opérationnel unique. Par exemple, si une organisation prend en charge 100 routeurs, il est important que les 100 routeurs soient configurés à l'aide des normes établies. Les normes de configuration des appareils sont définies dans la section technique de la politique de sécurité d'une organisation.

L'industrie de la sécurité informatique recommande aux DSI et aux chefs de projet un ensemble de standards et de bonnes pratiques pour réaliser leurs travaux de sécurisation des SI. L'application de ces normes garantit un cadre éprouvé et reconnu pour déployer une PSSI. L'écosystème le plus répandu est l'ensemble des normes 2700x. C'est l'outil indispensable avec lequel on vous propose de vous familiariser maintenant.

Tout d'abord, la famille de normes ISO 27000 est un recueil de bonnes pratiques dans le domaine de l'élaboration d'un système de management de la sécurité des SI (SMSI) et dans cette famille, il existe de nombreuses normes.

Normes	Date et révision	Descriptif	Lien avec la PSSI
ISO 27001	2005 – 2013	Ce standard définit les exigences à mettre en place pour l'élaboration d'un système de management de la sécurité de l'information. Basé sur l'amélioration continue de type « roue de Deming » Plan / Do / Check / Act, il précise les points de contrôle à respecter et propose dans son annexe A 114 mesures issues de l'ISO 27002.	C'est la base pour la mise en place d'un SMSI (système de management de la sécurité de l'information).
ISO 27002	2005 – 2013	Ce standard présente un guide de bonnes pratiques à mettre en œuvre pour des contrôles au regard des risques pesant sur l'information (confidentialité, intégrité et disponibilités). Il présente 114 mesures classées en 14 thèmes.	La méthodologie présentée dans le cours s'inspire directement des thèmes de l'ISO 27002 pour fixer les exigences et règles de sécurité.
ISO 27003	2010 – 2017	Cette norme présente un guide d'implémentation d'un SMSI. Il décrit le processus de conception.	Base pour la mise en place d'un SMSI.
ISO 27005	2008-2018	Cette norme se focalise sur la gestion des risques : définition du contexte, évaluation des risques, contrôle des résultats, révision. Par exemple, les méthodes EBIOS et MEHARI se basent de manière extensive sur la norme 27005.	Pas de lien direct, mais la PSSI se nourrit d'une analyse des risques qui peut s'appuyer sur l'ISO 27005. C'est même recommandé.

Tableau 2 : Normes de Sécurité

Les normes énoncent des principes essentiels, qui vont permettre un alignement progressif de la sécurité de l'information avec les meilleures pratiques de management : pilotage par les risques, formalisation des processus, contrôle, amélioration continue.

Pour autant, ces normes ne sont pas le Graal du RSSI :

- Elles n'aident pas à choisir le bon niveau de granularité et de détail pour conduire les analyses de risques ;
- Elles n'aident pas non plus à sélectionner les mesures de sécurité adaptées au contexte.

Il faut donc les envisager comme un référentiel d'objectifs, une proposition de méthodologie, qui doivent toutefois être enrichis du bon sens et de l'expertise des professionnels de la SSI. Seule cette combinaison assure la pertinence des choix d'implémentation.

4.3.7 Les enjeux et le champ d'application de la PSSI :

On doit fixer l'objet de la PSSI pour indiquer aux employés que le document :

- Fait référence spécifiquement à leur contexte de travail en termes de SSI
- Explicite les enjeux de sécurité pour l'activité de l'entreprise
- Présente les actions à mettre en œuvre pour amoindrir les risques.

Ensuite, on doit déterminer quelles sont les activités de l'entreprise qui rentrent dans le cadre de la PSSI. Pour définir un périmètre d'application, on doit se poser les questions suivantes :

- Quelles sont les activités de l'entreprise ?
- Comment celles-ci sont-elles organisées et coordonnées entre elles ?
- Quel est le degré de criticité pour chacune de ces activités, c'est-à-dire quelles activités pourraient mettre en danger la mission de l'entreprise, si leurs informations étaient compromises, indisponibles, volées, ou encore rendues publiques ?

Pour réaliser cette démarche, on doit garder en mémoire que l'objectif final est de fixer des exigences de sécurité pour améliorer le niveau de sécurité du SI. Pour faire une analyse des enjeux de sécurité, nous allons devoir demander en quoi la sécurité du SI est incontournable pour assurer le bon déroulement des activités de l'entreprise, en gardant à l'esprit que nous devons en déduire les exigences à respecter. Nous savons que le système d'information est au cœur des activités d'une entreprise donc il est important de souligner l'importance du SI pour la mission de l'entreprise et d'expliquer les conséquences sur la disponibilité, la confidentialité et l'intégrité des données du système.

La sécurité du système d'information constitue donc un axe de vigilance constant et d'action permanente. Chaque utilisateur est également un acteur de la sécurité du SI, et représente une priorité permanente pour l'administration de l'entreprise. Nous pouvons dire que chaque utilisateur est partie prenante de la sécurité et le système d'information est également susceptible d'accueillir des dispositifs innovants qui s'intègrent difficilement dans une gestion contraignante de la SSI. Une attention particulière doit être apportée aux règles de sécurité de

ces matériels. Il faut aussi noter que la politique de sécurité ne se limite pas à la protection contre la perte, l'indisponibilité ou la divulgation de données personnelles ou administratives, elle permet de créer un espace de confiance entre les professionnels et les clients.

4.3.8 Structure de rapport organisationnel :

Toutes les personnes d'une organisation, du chef de la direction (PDG) aux nouveaux employés, sont considérées comme des utilisateurs finaux du réseau et doivent se conformer à la politique de sécurité de l'organisation. L'élaboration et la maintenance de la politique de sécurité sont déléguées à des rôles spécifiques au sein du service informatique.

La direction au niveau exécutif doit toujours être consultée lors de la création de la politique de sécurité pour s'assurer que la politique est complète, cohérente et juridiquement contraignante. Les petites organisations peuvent avoir un seul poste de direction qui supervise tous les aspects de l'opération, y compris les opérations du réseau. Les grandes organisations peuvent diviser la tâche exécutive en plusieurs postes. La structure commerciale et hiérarchique d'une organisation dépend de sa taille et de son secteur d'activité.

La figure montre quatre membres d'une équipe de direction au niveau exécutif assis à une table de conférence participant à une réunion virtuelle avec d'autres membres.

4.3.8.1 Titres exécutifs communs :

Certains des titres exécutifs les plus courants incluent :

- Chief Executive Officer (CEO) : Responsable en dernier ressort du succès d'une organisation. Tous les postes de direction relèvent du PDG.
- Chief Technology Officer (CTO) : Identifie et évalue les nouvelles technologies. Dirige tout nouveau développement technologique. Responsable de l'entretien et de l'amélioration des systèmes existants. Fournit un leadership concernant toutes les questions liées à la technologie qui soutiennent les opérations. Le CTO est responsable de l'infrastructure technologique.
- Chief Information Officer (CIO) : Responsable de tous les systèmes informatiques et informatiques qui soutiennent les objectifs de l'entreprise. Dirige le déploiement réussi de nouvelles technologies et processus de travail. Dans les petites et moyennes organisations, ce rôle est souvent combiné avec le CTO. Le DSI assure le leadership lorsque des processus et des pratiques soutenant le flux d'informations sont élaborés.

- Chief Security Officer (CSO) : Développe, met en œuvre et gère la stratégie et les programmes de sécurité de l'organisation. Assure le leadership pour le développement de

tous les processus associés aux opérations commerciales, y compris la protection de la propriété intellectuelle. L'OSC doit limiter l'exposition à la responsabilité dans tous les domaines de risques financiers, physiques et personnels.

- Chief Information Security Officer (CISO) : Il se concentre spécifiquement sur la sécurité informatique. Le RSSI est responsable de l'élaboration et de la mise en œuvre de la politique de sécurité. Le RSSI peut être l'auteur principal de la politique de sécurité ou diriger d'autres auteurs. Dans tous les cas, le RSSI est responsable et responsable du contenu de la politique de sécurité.

4.3.9 Programme de sensibilisation à la sécurité :

La sécurité technique, administrative et physique est facilement violée si la communauté des utilisateurs finaux ne respecte pas délibérément les politiques de sécurité. Pour aider à assurer l'application de la politique de sécurité, un programme de sensibilisation à la sécurité doit être mis en place. Les dirigeants doivent développer un programme qui tient chacun au courant des problèmes de sécurité et informe le personnel sur la façon de travailler ensemble pour maintenir la sécurité de leurs données.

Un programme de sensibilisation à la sécurité reflète les besoins commerciaux d'une organisation tempérée par des risques connus. Il informe les utilisateurs de leurs responsabilités en matière de sécurité informatique et explique les règles de comportement pour l'utilisation des systèmes informatiques et des données au sein d'une entreprise. Ce programme doit expliquer toutes les politiques et procédures de sécurité informatique. Un programme de sensibilisation à la sécurité est essentiel au succès financier de toute organisation. Il diffuse les informations dont tous les utilisateurs finaux ont besoin pour mener efficacement leurs activités d'une manière qui protège l'organisation contre la perte de capital intellectuel, de données critiques et même d'équipement physique. Le programme de sensibilisation à la sécurité détaille également les sanctions que l'organisation impose en cas de non-conformité. Cette partie du programme devrait faire partie de toutes les orientations des nouveaux employés.

Un programme de sensibilisation à la sécurité comprend généralement deux éléments principaux :

- Campagnes de sensibilisation
- Formation

4.3.10 Les campagnes de sensibilisation :

Les campagnes de sensibilisation visent généralement tous les niveaux de l'organisation, y compris les postes de direction. Les efforts de sensibilisation à la sécurité visent à modifier les comportements ou à renforcer les bonnes pratiques de sécurité.

La sensibilisation n'est pas une formation. Le but des présentations de sensibilisation est simplement d'attirer l'attention sur la sécurité. Les présentations de sensibilisation visent à permettre aux individus de reconnaître les problèmes de sécurité informatique et d'y répondre en conséquence. Dans les activités de sensibilisation, l'apprenant est le destinataire de l'information. La sensibilisation repose sur l'atteinte d'un large public avec des techniques d'emballage attrayantes.

La protection antivirus est un exemple de sujet pour une session de sensibilisation ou de matériel de sensibilisation à distribuer. Le sujet peut être brièvement abordé en décrivant ce qu'est un virus, ce qui peut se passer si un virus infecte un système utilisateur, ce que l'utilisateur doit faire pour protéger le système et ce que les utilisateurs font s'ils découvrent un virus.

Il existe plusieurs méthodes pour accroître la sensibilisation à la sécurité :

- Lectures, vidéos
- Affiches, articles de newsletter et bulletins
- Récompenses pour les bonnes pratiques de sécurité
- Rappels, tels que des bannières de connexion, des tapis de souris, des tasses à café et des blocs-notes

4.3.11 Formations des utilisateurs :

La formation s'efforce d'enseigner les compétences de sécurité nécessaires aux utilisateurs finaux qui peuvent ou non être membres du personnel informatique. La différence la plus significative entre la formation et la sensibilisation est que la formation enseigne des compétences qui permettent à une personne d'effectuer une tâche spécifique, tandis que les campagnes de sensibilisation concentrent simplement l'attention d'une personne sur les problèmes de sécurité. Les compétences acquises par les utilisateurs au cours de la formation s'appuient sur les informations acquises lors des campagnes de sensibilisation à la sécurité. Suivre une campagne de sensibilisation à la sécurité avec des formations ciblées sur des publics spécifiques permet de consolider les informations et les compétences transmises.

Un exemple de cours de formation destiné au personnel non informatique est celui qui traite des pratiques de sécurité appropriées spécifiques aux applications que l'utilisateur final doit utiliser, telles que les applications de base de données. Un exemple de formation pour le

personnel informatique est un cours de sécurité informatique qui aborde en détail les contrôles de gestion, opérationnels et techniques qui doivent être mis en œuvre.

Un cours de formation à la sécurité efficace nécessite une planification, une mise en œuvre, une maintenance et une évaluation périodique appropriées. Le cycle de vie d'une formation à la sécurité comprend plusieurs étapes :

Étape 1. Identifier la portée, les buts et les objectifs du cours : Le champ d'application du cours fournit une formation à tous les types de personnes qui interagissent avec les systèmes informatiques. Étant donné que les utilisateurs ont besoin d'une formation directement liée à leur utilisation de systèmes particuliers, il est nécessaire de compléter un vaste programme à l'échelle de l'organisation par des cours plus spécifiques au système.

Étape 2. Identifier et former le personnel de formation : Il est important que les formateurs aient une connaissance suffisante des problèmes, principes et techniques de sécurité informatique. Il est également essentiel qu'ils sachent comment communiquer efficacement les informations et les idées.

Étape 3. Identifiez les publics cibles : Tout le monde n'a pas besoin du même degré ou du même type d'informations sur la sécurité informatique pour effectuer un travail assigné. Les cours de formation à la sécurité qui présentent uniquement les informations dont le public a besoin et omettent les informations non pertinentes donnent les meilleurs résultats.

Étape 4. Motiver la direction et les employés **:** Envisagez d'utiliser des techniques de motivation pour montrer à la direction et aux employés comment leur participation à un cours de formation profite à l'organisation

Étape 5. Administrer les formations : Les considérations importantes pour l'administration du cours comprennent la sélection des méthodes de formation, des sujets, du matériel et des techniques de présentation appropriés.

Étape 6. Mettre à jour les formations : Restez informé des changements dans la technologie informatique et les exigences de sécurité. Les cours de formation qui répondent aux besoins d'une organisation aujourd'hui peuvent devenir inefficaces lorsque l'organisation commence à utiliser une nouvelle application ou change son environnement, comme le déploiement de la VoIP.

Étape 7. Évaluer l'efficacité de la formation : Une évaluation vise à déterminer la quantité d'informations conservées, dans quelle mesure les procédures de sécurité informatique sont suivies et l'attitude générale à l'égard de la sécurité informatique.

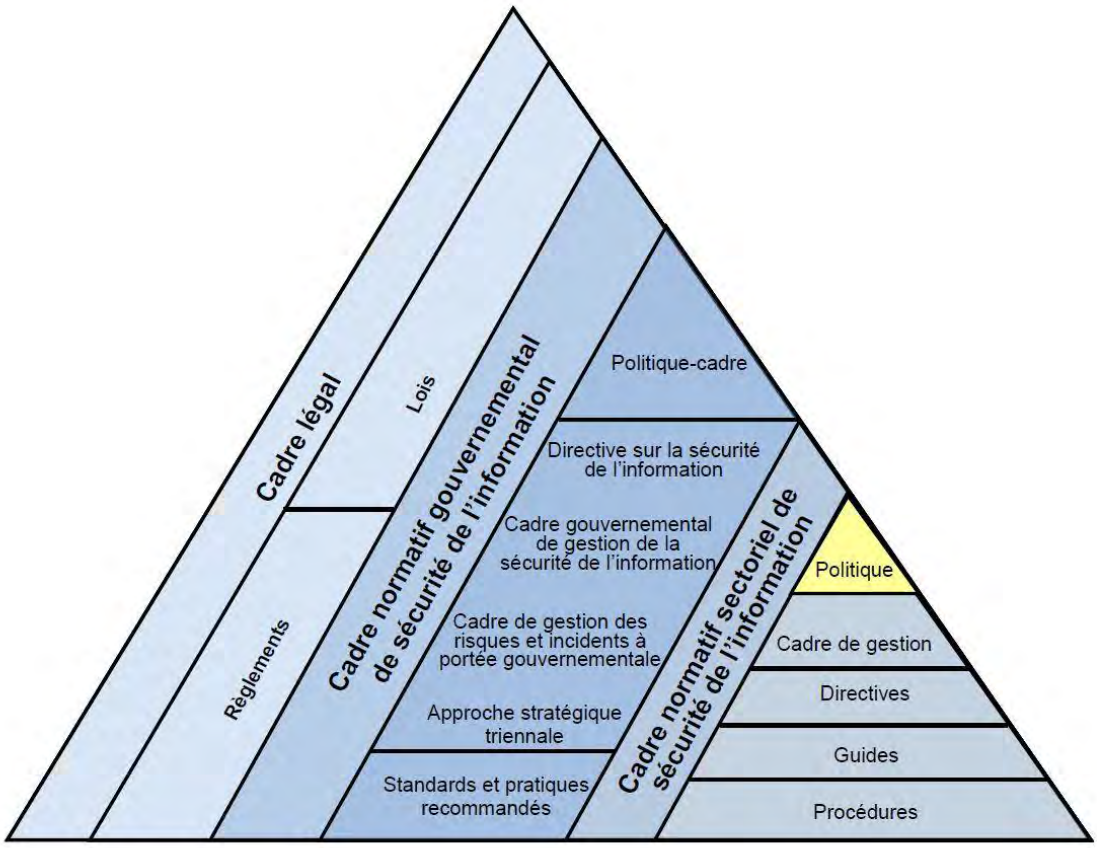

Figure 7 : Politique et cadre légal

3ième Partie : Mise en œuvre

Chapitre 5 : Politique de réglementation de l'usage du numérique en entreprise

La stratégie de la politique de sécurité est fondamentale dans un système informatique qui est un facteur déterminant de la performance (efficacité, efficience, maîtrise des risques) d'une organisation. Un SI inadapté ou mal maîtrisé peut-être une source de difficultés. Avec la digitalisation des processus, les entreprises manipulent de plus en plus des données à caractère personnel. C'est pourquoi l'entreprise doit avoir une politique de réglementation pour le respect de la vie privée.

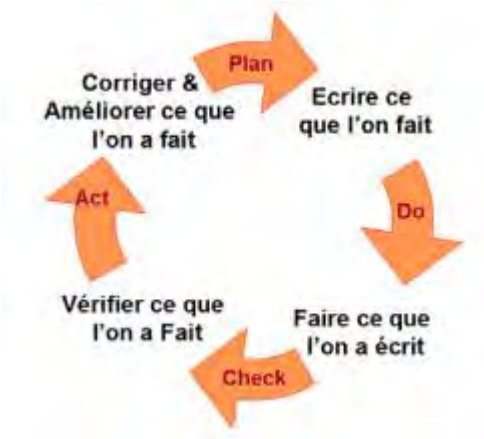

Figure 8 : Management de la sécurité du SI

5.1 Plan de continuité d'activité, parangon de la reprise après sinistre :

Face à l'informatisation croissante et à l'augmentation continue du nombre de menaces, les organisations comprennent de plus en plus aujourd'hui l'importance de mettre en place un plan de continuité d'activité (PCA). Mais, avant de se lancer dans la définition et la mise en œuvre de son PCA, il est nécessaire de prendre un peu de hauteur, de se poser les bonnes questions et de s'assurer que les conditions essentielles à son fonctionnement ont bel et bien été prises en compte.

5.1.1 L'intérêt d'un PCA :

Les organisations connaissent une informatisation croissante accompagnée d'un développement rapide des échanges avec leurs clients et partenaires, au travers de l'augmentation des flux externes, du développement des réseaux, et de l'attention accrue au service rendu à la clientèle ou aux usagers. Ce mouvement rend nécessaire, a minima, de mettre en place un dispositif de protection permettant d'assurer la continuité des missions essentielles de l'organisation. Les menaces pesant sur les Systèmes d'Information des entreprises sont nombreuses. Citons pour exemple les risques naturels (incendie, inondation, foudre, pandémie, etc.), les risques techniques (pollution logique, problème d'énergie, explosion, etc.), et les facteurs humains (erreur, malveillance, piratage, attentat, etc.).

De fait, mettre en place un plan de continuité d'activité dans son entreprise permet de contrer les risques majeurs. Son objectif est de réduire les risques d'indisponibilité de ressources (humaines, IT, etc.) et de discontinuité de service, par la mise en œuvre de moyens humains, techniques et organisationnels. Pour ce faire, il faut :

• Évaluer les risques majeurs d'indisponibilité : des locaux, des équipements, des moyens de communication, des personnes ;

• Définir une stratégie et un plan d'action face à ces risques : politique de prévention, organisation de la sécurité et mécanismes de continuité d'activité.

Mais, avant de se lancer dans la définition d'un plan de continuité d'activité, il est nécessaire de prendre un peu de hauteur et de vérifier que plusieurs conditions essentielles sont prises en compte :

• L'objectif du PCA doit être affirmé : par exemple, garantir la résilience des services critiques en cas de crise majeure (reste à définir ce qu'est une crise majeure dans le contexte de sa propre organisation) et/ou répondre à des attentes réglementaires, légales ou contractuelles ;

• L'adhésion par tous les acteurs doit être validée : le PCA a comme finalité, pour une entreprise, de survivre à une crise majeure, et ainsi d'assurer la pérennité de l'organisation (et de l'emploi de ses salariés…) à l'ensemble de ses collaborateurs. Pour autant, cette évidence doit être partagée par tous afin de permettre, le jour venu, une mise en œuvre opérationnelle réelle… ;

• Les bons moyens pourront être mis à disposition : la majorité des ressources déployées pour un PCA sont classiquement identifiées comme « non-productives ». C'est pourquoi, il est nécessaire de s'assurer de la capacité de l'organisation à soutenir les investissements nécessaires permettant au PCA d'être raisonnablement dimensionné, maintenu à jour et, si besoin, activé à tout moment avec les solutions initialement définies.

Ces conditions sont particulièrement à prendre en compte par la Direction générale de l'entreprise, afin d'assurer au porteur du PCA (appelons-le « RPCA » pour Responsable du PCA) le support nécessaire dans le déploiement de ce projet structurant et ambitieux ! Sans ce soutien, il sera difficile au RPCA de mettre en œuvre le bon PCA pour l'organisation.

5.1.2 La stratégie :

A titre d'illustration, la Figure ci-dessous reprend un exemple classique d'organisation d'un plan de continuité d'activité. Il est à noter que cette décomposition complète et précise doit être adaptée en fonction des enjeux, des attentes et/ou des moyens techniques et organisationnels de chaque entité.

Figure 9 : PCA

Nous ne nous attarderons pas sur le détail de chaque partie, mais les jalons critiques à retenir sont les suivants :

• Formaliser la stratégie de continuité d'activité ;

• Identifier et déployer les mécanismes de continuité (technique, humain, etc.) à mettre en œuvre ;

• Formaliser les procédures utiles à l'activation de tout ou partie du PCA ;

• Maintenir le PCA en condition opérationnelle ;

• Préparer les acteurs du PCA au travers de tests et d'exercices

Par ailleurs, et pour ceux qui ne savent pas par où commencer, la littérature sur le sujet est relativement importante et de nombreux documents permettent de démarrer un PCA selon une bonne méthodologie. Citons pour exemple (liste non exhaustive) :

• La norme ISO 22301 : 2019 décrivant les exigences d'un Système de management de la continuité d'activité (SMCA) et permettant de certifier une organisation en matière de continuité d'activité, sur un périmètre donné ;

• Le document « Cellules de crises et SI », publié par le CLUSIF en janvier 2017 ayant pour vocation de mettre à disposition du lecteur une série de repères, établis suivant l'état de l'art, pour l'aider à organiser la gestion d'une crise sur son SI.

• Le « Guide pour réaliser un plan de continuité d'activité », publié par le SGDSN, proposant une démarche méthodologique permettant l'élaboration concrète d'un plan de continuité d'activité.

5.1.2.1 Formaliser la stratégie de continuité d'activité ?

Pour ce faire, il faut :

• Se mettre d'accord sur la terminologie employée et les définitions qui en découlent : en continuité d'activité (comme ailleurs), de nombreux acronymes sont utilisés et lorsque l'on demande à plusieurs personnes la définition de ces acronymes, il est fréquent que ces dernières soient différentes ;

• Identifier le périmètre et les scenarii que l'on souhaite couvrir ;

• Identifier les risques pesant sur l'organisation (sur le périmètre retenu) ;

• Identifier les critères de reprise (au travers du BIA – Business Impact Analysis) et en particulier :

- le RTO (Recovery Time Objective) identifiant les délais sous lesquels devraient redémarrer les applications (des + au – critiques),
- le RPO (Recovery Point Objective) identifiant l'acceptation de perte de données,
- la montée en charge des utilisateurs identifiant combien de personnes sont attendues à un instant t pour assurer la reprise d'activité.

5.1.2.2 Identifier et déployer les mécanismes de continuité

La continuité d'activité s'appuie sur des ressources identifiées lors de l'étape précédente. Ces ressources peuvent être :

• Humaines : cœur de métier, métier support dont l'informatique ;

• Techniques : informatique centrale, PC utilisateurs, locaux, matériels spécifiques, etc. Du côté « humain », il s'agira principalement d'identifier les personnes qui interviendront le jour du sinistre et leur timing d'arrivée, à la fois côté SI et côté utilisateur, mais aussi celles qui seront à l'écart de la reprise. Côté technique, l'objectif sera notamment d'identifier les technologies à mettre en place (sauvegarde, réplication asynchrone ou synchrone, cluster, connexion à distance via un VPN, etc.), et de déployer celles qui sont nécessaires (préparation d'un site de secours, de PC utilisateurs, etc.).

Ce chantier est souvent le plus coûteux lorsque rien ou presque n'existe déjà au sein de l'organisation puisqu'il nécessite des investissements importants en propre ou via un prestataire spécialisé.

5.1.2.3 Formaliser les procédures utiles à l'activation de tout ou partie du PCA

Cette phase est particulièrement importante, pourtant dans les organisations ayant déjà déployé des mécanismes de reprise technique, elle est (assez) souvent oubliée… Il s'agit ici de formaliser les procédures qui permettront le jour du sinistre de ne pas se poser de mauvaises questions : « Où est le n° de téléphone de… ? », « J'interviens sur le PCA, mais je ne sais pas où je dois me rendre, ni qui appeler », « Comment puis-je restaurer le système de base de données, d'annuaire ?»

Bien entendu, les procédures ne répondent pas à tout et ne croyez pas ceux qui vous vendent un PCA clé-en-main tout prêt sur étagère : ils vous feraient prendre des vessies pour des lanternes. Les procédures de continuité d'activité ne s'improvisent pas ; pour être adaptées à 'organisation, elles demandent une expertise rigoureuse, du temps et des moyens !

Alors, ces procédures permettront de robotiser un certain nombre de tâches et de fiabiliser les données utiles à la reprise d'activités. De fait, elles sont indispensables et doivent être formalisées avec soin en prenant en compte les spécificités de l'organisation.

Ces procédures s'appliquent à l'ensemble des différents plans identifiés en Figure 1 : Plan de Gestion de Crise (PGC), Plan de Communication (PCOM), Plan de Reprise Métier (PRM, y compris le repli des utilisateurs), Plan de Continuité Informatique et Télécoms (PCIT) et Plan de Retour à la Normale (PRN). Les écarts (qui ne manqueront pas d'arriver !) avec les plans formalisés et la réalité de la crise seront quant à eux traités en direct par la Cellule de crise.

5.1.2.4 Maintenir le PCA en condition opérationnelle

Bien entendu, le Système d'Information de l'organisation vit et évolue au fil du temps. De ce fait, le PCA doit également évoluer. Ainsi, il est nécessaire de formaliser le cycle de vie des documents liés au PCA, en identifiant :

• La politique de révision des BIA (fréquence, périmètre) ;

• La prise en compte de nouveaux scenarii ;

• Les entrées/sorties des personnes impliquées dans le PCA (gestion des annuaires liés au PCA) ;

• Les évolutions (mineures et majeures) du Système d'Information (gestion de l'obsolescence des procédures techniques) ;

• Les évolutions de l'organisation (acquisition, cession, organigramme), les changements de sites, de locaux ;

• Etc.

5.1.2.5 Préparer les acteurs du PCA au travers de tests et d'exercices

Enfin, après avoir passé beaucoup de temps à la mise en place des mécanismes de continuité d'activité, il est temps de vérifier que tout cela fonctionne ! Pour ce faire, rien de tel que des tests et exercices, permettant de valider que les hommes et les femmes, ainsi que la technique sont opérationnels et prêts à réagir en temps de crise… et d'activation de tout ou partie du PCA.

Parmi les alternatives existantes, il est possible d'organiser des exercices de simulation de crise permettant de valider les réactions de la cellule de crise de l'organisation, des tests de bascules techniques (tout ou partie du PCIT), des exercices de repli utilisateurs, ou des exercices combinant 2 ou 3 de ces items.

5.2. Politique de réglementation de l'usage du numérique en entreprise :

Figure 10 : Management de la sécurité du système d'information

5.2 Elaboration de la politique de réglementation de l'usage numérique :

5.2.1 Politique de sécurité de l'information :

Il s'agit de définir les orientations de la direction en matière de sécurité de l'information. Les politiques de sécurité de l'information doivent être revues à intervalles programmés ou en cas de changements majeurs pour garantir leur pertinence, leur adéquation et leur effectivité dans le temps.

5.2.2 Organisation de la sécurité

L'organisation de la sécurité de l'information permet d'établir un cadre de gestion pour engager et vérifier la mise en œuvre et le fonctionnement de la sécurité de l'information au sein de l'organisation. Pour bien gérer l'organisation :

-Toutes les responsabilités en matière de sécurité de l'information doivent être définies et attribuées.

-Les tâches et les domaines de responsabilité incompatibles doivent être cloisonnés pour limiter les possibilités de modification ou de mauvais usage, non autorisé(e) ou involontaire, des actifs de l'organisation.

-Des relations appropriées avec les autorités compétentes doivent être entretenues.

-Des relations appropriées avec des groupes d'intérêt, des forums spécialisés dans la sécurité et des associations professionnelles doivent être entretenues.

-La sécurité de l'information doit être considérée dans la gestion de projet, quel que soit le type de projet concerné.

L'organisation de la sécurité de l'information permet également d'assurer la sécurité les activités nomades hors du périmètre physique de l'organisation telles le télétravail et l'utilisation d'appareils mobiles.

- Une politique et des mesures de sécurité complémentaires doivent être adoptées pour gérer les risques découlant de l'utilisation des appareils mobiles.

- Une politique et des mesures de sécurité complémentaires doivent être mises en œuvre pour protéger les informations consultées, traitées ou stockées dans l'environnement de télétravail.

5.2.3 La sécurité des ressources humaines

La sécurité des ressources humaines consiste à s'assurer que les collaborateurs comprennent leurs responsabilités en matière de sécurité de l'information, qu'ils en sont conscients et qu'ils les assument. Les intérêts de l'organisation demeurent protégés dans le cadre du processus de modification, de rupture ou de terme d'un contrat de travail.

-Avant l'embauche : Il faut s'assurer que les employés et les contractants comprennent leurs responsabilités et qu'ils sont compétents pour remplir les fonctions que l'organisation envisage de leur confier. Des vérifications doivent être effectuées sur tous les candidats à l'embauche conformément aux lois, aux règlements et à l'éthique et être proportionnées aux exigences métier, à la classification des informations accessibles et aux risques identifiés. Les accords contractuels entre les employés et les sous-traitants doivent préciser leurs responsabilités et celles de l'organisation en matière de sécurité de l'information.

- Lors du mandat de l'individu : la direction doit demander à tous les employés et sous-traitants d'appliquer les règles de sécurité de l'information conformément aux politiques et aux procédures en vigueur dans l'organisation. L'ensemble des employés de l'organisation et des sous-traitants doivent bénéficier d'une sensibilisation et de formations adaptées. Ils doivent aussi recevoir régulièrement les mises à jour des politiques et procédures de l'organisation s'appliquant à leurs fonctions. Un processus disciplinaire formel et connu de tous doit exister pour prendre des mesures à l'encontre des employés ayant enfreint les règles liées à la sécurité de l'information.

- A la fin du contrat : on doit vérifier que tous les équipements sont retournés et que les droits d'accès sont retirés. Les responsabilités et les missions liées à la sécurité de l'information qui restent valables à l'issue de la rupture du contrat doivent être définies, communiquées aux employés ou sous-traitants.

5.2.4 Gestion des actifs

La gestion des actifs informationnels est primordiale. L'organisation doit identifier ses actifs et définir les responsabilités afin de s'assurer qu'ils bénéficient d'un niveau de protection adéquat conforme à son importance pour l'activité. La divulgation, la modification et la destruction d'informations, non autorisées doivent être empêchées. Les actifs associés à l'information et aux moyens de traitement de l'information doivent être identifiés et un inventaire de ces actifs doit être dressé et tenu à jour. Les actifs figurant à l'inventaire doivent être attribués à un propriétaire. Les règles d'utilisation correcte de l'information, les actifs associés à l'information et les moyens de traitement de l'information doivent être identifiés, documentés et mis en œuvre. Tous les utilisateurs tiers doivent restituer la totalité des actifs de l'organisation qu'ils ont en leur possession au terme du contrat.

Ces actifs peuvent être :

- Des biens physiques (serveurs, réseau, imprimantes, baies de stockage, poste de travail, des matériels non IT)

- Des informations (base de données, fichiers, archives)
- Des logiciels (application ou dispositif)
- Des services
- De la documentation (politiques, procédures, plans)

5.2.5 Contrôle d'accès

Le contrôle d'accès permet de maîtriser l'accès utilisateur par le biais de privilèges et empêcher les accès non autorisés aux systèmes, aux applications et aux services d'information. Les utilisateurs sont responsables de la protection de leurs informations d'authentification.

En matière de contrôle d'accès, une politique doit être établie, documentée et revue sur la base des exigences métier. Les utilisateurs doivent avoir uniquement accès au réseau et aux services pour lesquels ils ont spécifiquement reçu une autorisation.

Concernant la gestion de l'accès utilisateur :

- Un processus formel d'enregistrement des utilisateurs doit être mis en œuvre pour permettre l'attribution des droits d'accès.
- Un processus formel de distribution des accès aux utilisateurs doit être mis en œuvre pour attribuer et retirer des droits d'accès à tous types d'utilisateurs sur l'ensemble des services et des systèmes.
- L'allocation et l'utilisation des droits d'accès à privilèges doivent être restreintes et contrôlées
- L'attribution des informations secrètes d'authentification doit être réalisée dans le cadre d'un processus de gestion formel.
- Les propriétaires d'actifs doivent vérifier les droits d'accès des utilisateurs à intervalles réguliers.
- Les droits d'accès aux informations et aux moyens de traitement des informations de l'ensemble des utilisateurs tiers doivent être retirés à la fin de leur période d'emploi, ou adaptés en cas de modification du contrat.

Concernant les responsabilités des utilisateurs :

- Les utilisateurs doivent suivre les pratiques de l'organisation pour l'utilisation des informations secrètes d'authentification.

Concernant le contrôle de l'accès au système et à l'information :

- L'accès à l'information et aux fonctions d'application système doit être restreint conformément à la politique de contrôle d'accès.
- Lorsque la politique de contrôle d'accès l'exige, l'accès aux systèmes et aux applications doit être contrôlé par une procédure de connexion sécurisée.

- Les systèmes qui gèrent les mots de passe doivent être interactifs et doivent garantir la qualité des mots de passe.
- L'utilisation des programmes utilitaires permettant de contourner les mesures de sécurité d'un système ou d'une application doit être limitée et étroitement contrôlée.
- L'accès au code source des programmes doit être restreint.

5.2.6 Cryptographie

La cryptographie permet de protéger la confidentialité, l'authenticité et l'intégrité de l'information mais son utilisation doit être correcte et efficace.

Ce pendant des mesures cryptographiques sont définies :

- Une politique sur l'utilisation des mesures cryptographiques en vue de protéger l'information doit être élaborée.
- Une politique sur l'utilisation, la protection et la durée de vie des clés cryptographiques doit être mise en œuvre tout au long de leur cycle de vie.

5.2.7 Sécurité physique et environnementale

La sécurité physique et environnementale prévient tout accès physique non autorisé, tout dommage ou intrusion portant sur l'information et les moyens de traitement de l'information de l'organisation. Elle vise à empêcher la perte, l'endommagement, le vol ou la compromission des actifs et l'interruption des activités de l'organisation.

Concernant les zones à sécuriser :

- Des périmètres de sécurité doivent être définis et utilisés pour protéger les zones contenant l'information sensible ou critique et les moyens de traitement de l'information.
- Les zones doivent être protégées par des contrôles adéquats à l'entrée pour s'assurer que seul le personnel autorisé est admis.
- Des mesures de sécurité physique aux bureaux, aux salles et aux équipements doivent être conçues et appliquées.
- Des mesures de protection physique contre les désastres naturels, les attaques malveillantes ou les accidents doivent être conçues et appliquées.
- Des procédures pour le travail dans les zones sécurisées doivent être conçues et appliquées.
- Les points d'accès tels que les zones de livraison et de chargement et les autres points par lesquels des personnes non autorisées peuvent pénétrer dans les locaux doivent être contrôlés et, si possible, isolés des moyens de traitement de l'information, de façon à éviter les accès non autorisés.

Pour les matériels :

- Les matériels doivent être localisés et protégés de manière à réduire les risques liés à des menaces et des dangers environnementaux et les possibilités d'accès non autorisé.
- Les matériels doivent être protégés des coupures électriques et d'autres perturbations dues à une défaillance des services généraux.
- Les câbles électriques ou de télécommunication transportant des données ou supportant les services d'information doivent être protégés contre toute interception ou tout dommage.
- Les matériels doivent être entretenus correctement pour garantir leur disponibilité permanente et leur intégrité.
- Les matériels, les informations ou les logiciels des locaux de l'organisation ne doivent pas sortir sans autorisation préalable.
- Des mesures de sécurité doivent être appliquées aux matériels utilisés hors des locaux de l'organisation en tenant compte des différents risques associés au travail hors site.
- Tous les composants des matériels contenant des supports de stockage doivent être vérifiés pour s'assurer que toute donnée sensible a bien été supprimée et que tout logiciel sous licence a bien été désinstallé ou écrasé de façon sécurisée, avant leur mise au rebut ou leur réutilisation.
- Les utilisateurs doivent s'assurer que les matériels non surveillés sont dotés d'une protection appropriée.
- Une politique de gestion des documents papier et des supports de stockage amovibles et de verrouillage des équipements des moyens de traitement de l'information, doivent être adoptées.
- Les procédures d'exploitation doivent être documentées et mises à disposition de tous les utilisateurs concernés.
- Les changements apportés à l'organisation, aux processus métier, aux systèmes et moyens de traitement de l'information ayant une incidence sur la sécurité, doivent être contrôlés.
- L'utilisation des ressources doit être surveillée et ajustée et des projections sur les dimensionnements futurs doivent être effectuées pour garantir les performances exigées du système.
- Les environnements de développement, de test et d'exploitation doivent être séparés pour réduire les risques d'accès ou de changements non autorisés dans l'environnement d'exploitation.

Pour la protection contre les logiciels malveillants :

- Des mesures de détection, de prévention et de récupération conjuguées à une sensibilisation des utilisateurs adaptée, doivent être mises en œuvre pour se protéger contre les logiciels malveillants.

Pour la sauvegarde :

- Des copies de sauvegarde de l'information, des logiciels et des images systèmes doivent être réalisés et testés régulièrement conformément à une politique de sauvegarde convenue.

Pour la journalisation et surveillance :

- Des journaux d'événements enregistrant les activités de l'utilisateur, les exceptions, les défaillances et les événements liés à la sécurité de l'information doivent être créés, tenus à jour et vérifiés régulièrement.
- Les moyens de journalisation et d'information journalisée doivent être protégés contre les risques de falsification ou d'accès non autorisé.
- Les activités de l'administrateur système et de l'opérateur système doivent être journalisées, protégées et vérifiées régulièrement.
- Les horloges de l'ensemble des systèmes de traitement de l'information concernés d'une organisation ou d'un domaine de sécurité doivent être synchronisées sur une source de référence temporelle unique.

Pour la maîtrise des logiciels d'exploitation :

- Des procédures doivent être mises en œuvre pour contrôler l'installation de logiciel sur des systèmes en exploitation.

Pour la gestion des vulnérabilités techniques :

- Des informations sur les vulnérabilités techniques des systèmes d'information en exploitation doivent être obtenues en temps opportun. L'exposition de l'organisation à ces vulnérabilités doit être évaluée et les mesures appropriées doivent être prises pour traiter le risque associé.
- Des règles régissant l'installation de logiciels par les utilisateurs doivent être établies et mises en œuvre.

Pour les considérations sur l'audit des systèmes d'information :

- Les exigences et activités d'audit impliquant des vérifications sur des systèmes en exploitation doivent être prévues avec soin et validées afin de réduire au minimum les perturbations subies par les processus métier.

5.2.8 Sécurité liée à l'exploitation

La sécurité de l'exploitation permet de s'assurer que l'information et les moyens de traitement de l'information sont protégés contre les logiciels malveillants. Elle garantit l'intégrité des systèmes en exploitation et empêche toute exploitation des vulnérabilités techniques.

Pour cela il convient de créer, documenter et de diffuser des procédures d'exploitation.

5.2.9 Sécurité des communications

La sécurité des communications protège l'information qui transite via les réseaux et à travers les infrastructures informatiques utilisées pour assurer cette sécurité. Elle maintient la sécurité de l'information circulant à l'intérieur et à l'extérieur de l'organisation.

Pour la gestion de la sécurité des réseaux :

- Les réseaux doivent être gérés et contrôlés pour protéger l'information contenue dans les systèmes et applications.
- Pour tous les services de réseau, les mécanismes de sécurité, les niveaux de service et les exigences de gestion, doivent être identifiés et intégrés dans les accords de services de réseau, que ces services soient fournis en interne ou externalisés.
- Les groupes de services d'information, d'utilisateurs et de systèmes d'information doivent être cloisonnés sur les réseaux.

Pour le transfert de l'information :5

- Des politiques, des procédures et des mesures de transfert formelles doivent être mises en place pour protéger les transferts d'information transitant par tous types d'équipements de communication.
- Des accords doivent traiter du transfert sécurisé de l'information liée à l'activité entre l'organisation et les tiers.
- L'information transitant par la messagerie électronique doit être protégée de manière appropriée.
- Les exigences en matière d'engagement de confidentialité ou de non-divulgation, doivent être identifiées, vérifiées régulièrement et documentées conformément aux besoins de l'organisation.

5.2.10 Acquisition, développement et maintenance des systèmes d'information

Pour que la sécurité de l'information soit mise en œuvre efficacement, les exigences de sécurité à satisfaire lors de l'acquisition, du développement, de la mise en place et de la maintenance d'un actif informationnel, doivent être déterminées. Les exigences de sécurité doivent tenir compte de l'évolution des technologies et des nouveaux enjeux.

Pour les exigences de sécurité applicables aux systèmes d'information :

- Les exigences liées à la sécurité de l'information doivent être intégrées aux exigences des nouveaux systèmes d'information ou des améliorations de systèmes d'information existants.

- Les informations liées aux services d'application transmises sur les réseaux publics doivent être protégées contre les activités frauduleuses, les différents contractuels, ainsi que la divulgation et la modification non autorisées.
- Les informations impliquées dans les transactions liées aux services d'application doivent être protégées pour empêcher une transmission incomplète, des erreurs d'acheminement, la modification, la divulgation et la duplication non autorisées du message.

Pour la Sécurité des processus de développement et d'assistance technique :

- Des règles de développement des logiciels et des systèmes doivent être établies et appliquées au développement de l'organisation.
- Les changements des systèmes dans le cadre du cycle de développement doivent être contrôlés par le biais de procédures formelles.

- Lorsque des changements sont apportés aux plateformes d'exploitation, les applications critiques métier doivent être vérifiées et testées afin de détecter l'absence de tout effet indésirable sur l'activité ou sur la sécurité.
- Les modifications des progiciels ne doivent pas être encouragées et limitées aux changements nécessaires.
- Des principes d'ingénierie de la sécurité des systèmes doivent être établis, documentés, tenus à jour et appliqués à tous les travaux de mise en œuvre des systèmes d'information.
- Les organisations doivent établir des environnements de développement sécurisés pour les tâches de développement et d'intégration du système, qui englobe l'intégralité du cycle de vie du développement du système, et en assurer la protection de manière appropriée.
- L'organisation doit superviser et contrôler l'activité de développement du système externalisée.
- Les tests de fonctionnalité de la sécurité doivent être réalisés pendant le développement.
- Des programmes de test de conformité et des critères associés doivent être déterminés pour les nouveaux systèmes d'information, les mises à jour et les nouvelles versions.

Pour les données du test :

- Les données de test doivent être sélectionnées avec soin, protégées et contrôlées.

5.2.11 Relations avec les fournisseurs

La sécurité liée aux relations avec les fournisseurs vise à garantir la protection des actifs de l'organisation accessibles aux fournisseurs. Elle assure également le maintien du niveau

convenu de sécurité de l'information et de prestation de services, conformément aux accords conclus avec les fournisseurs.

Pour la Sécurité dans les relations avec les fournisseurs :

- Des exigences de sécurité de l'information pour limiter les risques résultant de l'accès des fournisseurs aux actifs de l'organisation doivent être formelles.
- Les exigences applicables liées à la sécurité de l'information doivent être établies et convenues avec chaque fournisseur pouvant accéder, traiter, stocker, communiquer ou fournir des composants de l'infrastructure informatique destinés à l'information de l'organisation.
- Les accords conclus avec les fournisseurs doivent inclure des exigences sur le traitement des risques liés à la sécurité de l'information associé à la chaîne d'approvisionnement des produits et des services informatiques.

Pour la Gestion de la prestation du service :

- Les organisations doivent surveiller, vérifier et auditer à intervalles réguliers la prestation des services assurés par les fournisseurs.
- Le Fournisseur de services est tenu de mettre en œuvre l'ensemble des mesures techniques et organisationnelles appropriées, y compris celles spécifiées dans le contrat, de sorte que le traitement des Données personnelles soit conforme aux exigences du respect de la vie privée.
- Les changements effectués dans les prestations de service des fournisseurs, comprenant le maintien et l'amélioration des politiques, procédures et mesures existant en matière de sécurité de l'information, doivent être gérés en tenant compte du caractère critique de l'information, des systèmes et des processus concernés et de la réappréciation des risques.

5.2.12 Gestions des incidents liés à la sécurité

La gestion des incidents de sécurité de l'information doit s'appuyer sur une méthode cohérente et efficace, incluant la communication des événements et des failles de sécurité.

- Des responsabilités et des procédures permettant de garantir une réponse rapide, efficace et pertinente doivent être établies en cas d'incident lié à la sécurité de l'information.
- Les événements liés à la sécurité de l'information doivent être signalés dans les meilleurs délais par les voies hiérarchiques appropriées.
- Les employés et les sous-traitants utilisant les systèmes et services d'information de l'organisation doivent noter et signaler toute faille de sécurité observée ou soupçonnée dans les systèmes ou services.
- Les événements liés à la sécurité de l'information doivent être appréciés et il doit être décidé s'il faut les classer comme incidents liés à la sécurité de l'information.

- Les incidents liés à la sécurité de l'information doivent être traités conformément aux procédures documentées.
- Les connaissances recueillies suite à l'analyse et la résolution d'incidents doivent être utilisées pour réduire la probabilité ou l'impact d'incidents ultérieurs.
- L'organisation doit définir et appliquer des procédures d'identification, de collecte, d'acquisition et de protection de l'information pouvant servir de preuve.

5.2.13 Aspects de la sécurité de l'information dans la Gestion de la continuité de l'activité

La continuité de la sécurité de l'information doit être la partie intégrante des systèmes de gestion de la continuité de l'activité. Elle vise à garantir la disponibilité des moyens informatiques.

Pour la continuité de la sécurité de l'information :

- L'organisation doit déterminer ses exigences en matière de sécurité de l'information et de continuité de management de la sécurité de l'information dans des situations défavorables, comme lors d'une crise ou d'un sinistre
- L'organisation doit établir, documenter, mettre en œuvre et tenir à jour des processus, des procédures et des mesures permettant de fournir le niveau requis de continuité de sécurité de l'information au cours d'une situation défavorable.
- L'organisation doit vérifier les mesures de continuité de la sécurité de l'information mises en œuvre à intervalles réguliers afin de s'assurer qu'elles sont valables et efficaces dans des situations défavorables.

Pour les redondances :

- Des moyens de traitement de l'information doivent être mis en œuvre avec suffisamment de redondances pour répondre aux exigences de disponibilité.

5.2.14 Conformité

La conformité a pour but d'éviter toute violation des exigences et obligations légales, statutaires, réglementaires ou contractuelles relatives à la sécurité de l'information. Elle doit garantir une sécurité mise en œuvre et appliquée conformément aux politiques et procédures organisationnelles.

Pour la conformité aux obligations légales et réglementaires :

- Toutes les exigences légales, statutaires, réglementaires et contractuelles en vigueur, ainsi que l'approche adoptée par l'organisation pour satisfaire à ces exigences, doivent être explicitement définies, documentées et mises à jour pour chaque système d'information.

- Des procédures appropriées doivent être mises en œuvre pour garantir la conformité avec les exigences légales, réglementaires et contractuelles relatives à la propriété intellectuelle et à l'usage des licences de logiciels propriétaires.
- Les enregistrements doivent être protégés de la perte, de la destruction, de la falsification, des accès non autorisés et des diffusions non autorisées, conformément aux exigences légales, réglementaires, contractuelles et aux exigences métier.
- La protection des données à caractère personnel et de la vie privée doit être garanties telles que l'exigent la législation ou les réglementations applicables, et les clauses contractuelles le cas échéant.
- Des mesures cryptographiques doivent être prises conformément aux accords, législation et réglementations applicables.

Pour la revue de la sécurité de l'information :

- Des revues régulières et indépendantes de l'approche retenue par l'organisme pour gérer et mettre en œuvre la sécurité de l'information (le suivi des objectifs de sécurité, les mesures, les politiques, les procédures et les processus relatifs à la sécurité de l'information) doivent être effectuées à intervalles définis ou lorsque des changements importants sont intervenus.
- Les responsables doivent régulièrement vérifier la conformité du traitement de l'information et des procédures dont ils sont chargés au regard des politiques, des normes de sécurité applicables et autres exigences de sécurité.
- Les systèmes d'information doivent être examinés régulièrement quant à leur conformité avec les politiques et les normes de sécurité de l'information de l'organisation.

Figure 11 : Protection et Prévention d'un organisme

Conclusion et Perspective

L'objet de ce mémoire était de mettre en place une politique de réglementation de l'usage du numérique en entreprise qui s'est introduit à un rythme effréné dans nos vies privées et professionnelles.

Actuellement toute entreprise adoptant la digitalisation doit être consciente des risques et avoir une politique pour sensibiliser les employés sur les principes et les attitudes afin de bien protéger le système d'information de l'entreprise.

Réaliser ce travail a été très bénéfique car il nous a permis de faire des recherches sur le système de management de la sécurité de l'information, sur la gestion des risques, sur l'identité numérique, sur le plan de continuité d'activité et surtout d'approfondir nos connaissances acquises en classe. En effet, nous avons passé en revue nos cours d'audit sécurité pour pouvoir mettre en place cette politique.

L'essentiel pour nous était d'étudier, de comprendre et de mettre en place une politique de réglementation de l'usage du numérique pour d'assurer la protection des données personnelles et de la vie privée des employés et clients de l'entreprise. Cette étude nous a ouvert plusieurs pistes de réflexion et que nous allons continuer à développer.

Cependant, ce thème reste un sujet d'actualité et fait l'objet de nombreux débats. Certaines perspectives peuvent s'orienter dans le sens de trouver d'autres stratégies pour gérer la continuité d'activité et la reprise d'activité de l'entreprise en cas de sinistre.

Bibliographie

2008-12 du 25 janvier 2008, CDP-Sénégal

La loi portant sur la Protection des données à caractère personnel

Iddri, FING, WWF France, GreenIT.fr (2018). Livre blanc Numérique et Environnement :

La révolution numérique dans les entreprises

OpenEdition Press 2013, Encyclopédie numérique, Marseille, 2014, Nombre de pages : 122 p.

Identité numérique

Cours de M. Modou Fall, Sécurité Réseau de, Chapitre 11 :

Politique de sécurité

Webographie

Sécurité informatique,

https://international.scholarvox.com/catalog/search / informatique?

(Consulté le 06/05/2020)

Solution pour une politique de sécurité,

https://www.netacad.com/courses/networking

(Consulté le 21/11/2020)

Les normes iso,

https://www.iso.org/obp/ui/fr/#iso:std:iso-iec:27002:ed-2:v1:fr

(Consulté le 02/11/2019)

La règlementation de l'usage du numérique dans les entreprises,

https://www.cdp.sn/content/loi-n%C2%B0-2008-12-du-25-janvier-2008-portant-sur-la-protection

(Consulté le 09/11/2019)

Table des matières