La sécurité des réseaux et des systèmes

Abdelaziz Sabri

Sommaire

1 Introduction 5

2 La vulnérabilité du système informatique 7

2.1 Définition : 7

2.2 Vulnérabilités informatiques : 7

3 Liste des risques de sécurité informatique 9

3.1 Physiques 9

3.2 Naturels 9

3.3 Rayonnements 9

3.4 Compromission des informations et des fonctions 9

3.5 Défaillance technique 10

3.6 Agression Physique, Erreur 11

4 Les types d'attaques sur un réseau 12

4.1 Les attaques d'accès 12

4.2 Le sniffing 12

4.3 Les chevaux de Troie 12

4.4 Porte dérobée 12

4.5 L'ingénierie sociale 13

4.6 Le craquage de mots de passe 13

4.7 Les attaques de modification 13

4.8 Virus, vers et chevaux de Troie 13

4.9 Les attaques par saturation (déni de service) 13

4.10 Le flooding 14

4.11 Le TCP-SYN flooding 14

4.12 Le smurf 14

4.13 Le débordement de tampon 14

4.14 Les attaques de répudiation 14

4.15 Le IP spoofing 14

4.16 watering hole ("Trou d'eau") 15

5 Liste de mesures à mettre en place 16

5.1 Mesures Physiques 16

5.2 Mesures Techniques 16

5.3 Organisation / Plan de sécurité 16
6 Introduction à la Sécurité d'un Réseau. 17
7 La Sécurité Physique. 17
8 Périmètre de la Sécurité Physique. 18
8.1 Sécurité physique des Locaux et Matériels. 18
Classifications des locaux 18
Identification des risques. 18
Salle Serveur 19
Locaux Techniques 19
8.2 Recommandations de Sécurité Physique. 19
8.2.1 La Localisation. 19
8.2.2 La Structure 20
8.3 L'Infrastructure Electrique. 20
8.3.1 L'Alimentation Electrique Générale 20
8.3.2 Le Groupe Electrogène. 21
8.3.3 Les Onduleurs. 21
8.3.4 Le Câblage Electrique. 21
8.4 La Climatisation. 22
8.5 La Protection Incendie. 22
8.6 Le Contrôle d'Accès. 22
8.7 La vidéo Surveillance. 23
9 La Sécurité Administrative. 23
9.1 Compte -Rendu d'alarme. 23
9.2 Compte -Rendu d'événements. 24
10 La Sécurité Logique 24
11 La Sécurité des Accès Logiques. 25
11.1 Intérêts de la Gestion des Identités et des Accès 25
11.2 La Gestion des Identités et des Accès 25
11.3 La responsabilité de l'Utilisateur 26
12 Le contrôle d'Accès au Réseau. 27
12.1 Règles d'utilisation, de sécurité et de bon usage 27
12.2 Les Pratiques à ne pas faires 28
13 La Sauvegardes des Données. 29
13.1 Déterminer l'information à sauvegarder 29

13.2 Médias de sauvegarde et d'archivage : 30
13.3 Stratégies de sauvegarde : 30
13.4 Modes de sauvegarde : 31
14 Que faire en cas d'incident 34
15 Plan de continuité d'activité 35
15.1 Organisation à mettre en Place. 37
15.2 Documentations. 37
15.3 Maintenance du Plan 38
15.4 Plan de Test 39
16 Mise en Place d'une Politique de sécurité 40
16.1 Introduction 40
16.2 Les recommandations générales 40
17 Historique et Evolutions des Normes en matière de sécurité de l'information 43

1 Introduction

La cybercriminalité, dont l'ampleur, la fréquence et la complexité ne cessent de croître, nous obligent à renforcer notre cyber sécurité. Cette prise de conscience est importante , elle nous permettra de protéger notre Patrimoine informationnelle et garantir la pérennité de nos systèmes.

Actuellement nous devons faire face non seulement à une délinquance informatique mais à de vraies organisations criminelles qui peuvent nuire aux entreprises et par conséquent à tous un pays.

Cette délinquance informatique organisée ou isolée profite à des organisations qui peuvent avoir des motivations différentes. La cybercriminalité a évolué vers le Cyber terrorisme qui peut avoir de graves conséquences économique.

On observe de plus en plus de systèmes industriels informatisé qui sont interconnecté au réseau IT de l'entreprise voir avec internet ,et on voit plus en plus de personnes s'intéresser à l'attaque de ces dispositifs .Il est absolument impérative que l'entreprise disposant de systèmes industriels vérifie bien les mécanismes de sécurités qui sont mis en place pour l'isolation avec internet .

Les meilleurs façons de se prémunir et de limiter l'impact d'une éventuelle cyber attaque , est de former et sensibiliser le personnels à organiser la défense de ces systèmes informatiques; Un effort pédagogique vital semble d'autant plus urgent à mettre en place que les groupes de cybercriminels développent régulièrement de nouvelles méthodes, mélange d'ingénierie sociale et de tour de force technique.

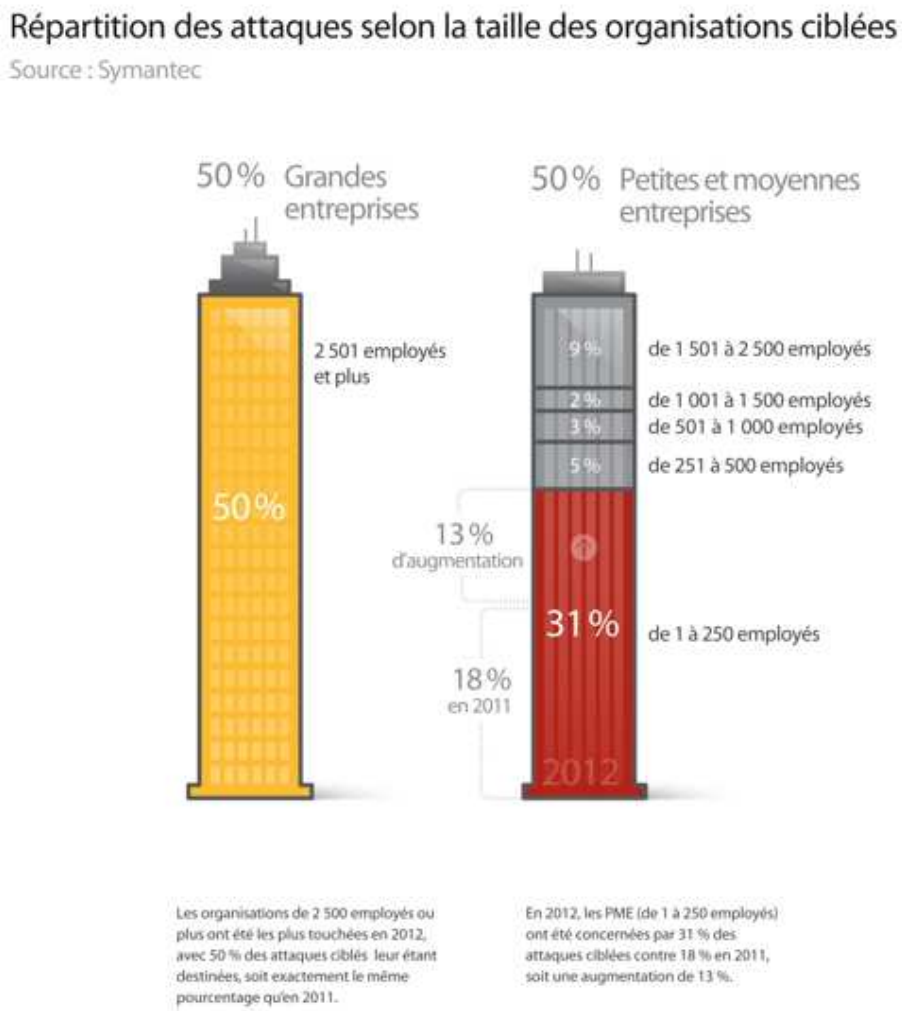
Quelque Chiffre Concernant la cyber sécurité pour l'année 2012 qui a vu exploser le nombre de cyber attaque nous montre l'ampleur de la situation

Les cyber attaques ont augmentés de 42% en 2012 et multipliées par trois entre 2011 et 2012.

Le rapport annuel de la société Symantec, publié en avril 2013, Montre :

- L'Année 2011 avait vu les ministères et services publics ciblés
- Année 2012 a vu la cible des cybercriminels se déplacer vers le monde industriel, notamment High tech et de la chimie, qui représente désormais 24% des attaques. « Conçues pour le vol de propriété intellectuelle, ces attaques de cyber-espionnage touchent de plus en plus le secteur industriel ainsi que les PME de moins de 250 salariés, qui sont la cible de 31% de ces attaques contre 18 % en 2011.

.



Quels Attaques:

- Attaque contre L'IRAN (Virus Le virus Stuxnet contre les systèmes informatiques industriels de l'iran)
- Attaque contre le système pétrolier saoudien ,visait son système SCADA de production de pétrole (Une cyber attaque qui a eu pour conséquence l'infection par un virus de 30.000 postes de travail.)
- Des hackers détournent 45 millions de dollars (Mai 2013) des attaques similaires en décembre 2012 et Février 2013

Cause Principale = infrastructure et pratiques de sécurité sont souvent inadéquates

2 La vulnérabilité du système informatique

2.1 Définition :

La vulnérabilité traduit la sensibilité d'un bien, d'une activité ou d'un territoire à la submersion. Ce terme regroupe toutes les atteintes directes (dommages évaluables) et indirectes (perturbations peu ou non évaluables)

La vulnérabilité est une faiblesse du système qui le rend sensible à une menace :

On distingue :

Vulnérabilité des systèmes et des applications :
Authentification, Mot de passe (et Droit d'accès)
Failles liées à la gestion de la pile : buffer overflow, format string
Failles liées à la gestion des processus : escalade des privilèges
Failles webs : SQL injection, etc

Vulnérabilité des réseaux *:*
Déjouer les principales attaques réseaux
Chiffrement et sécurité : authentification, non-répudation, notarisation, . . .
Firewall, DMZ, proxy et honypots
Outils d'attaques/défenses

2.2 Vulnérabilités informatiques :

Vulnérabilité informatique: erreur de conception (bug) dans un produit pouvant altérer la sécurité du système.

Où peut-on trouver des vulnérabilités ?

- ✓ Au niveau du système d'exploitation
- ✓ Au niveau applicatif
- ✓ Au niveau du réseau

Qui trouve des vulnérabilités ?

- ✓ Des chercheurs en vulnérabilités indépendants (Vulnerability Contributor Program d'iDEFENSE, fondation Mozilla,.)
- ✓ Des "chercheurs en vulnérabilités" dont c'est le métier, (eEye, NGS, ISS, Core-ST, Symantec, …)
- ✓ Plus rarement les éditeurs de logiciels.

Comment trouver les vulnérabilités ?

- ✓ Audit de code source
- ✓ Tests sur le produit
- ✓ Reverse-engineering
- ✓ etc.

Que faire ensuite ?

- ✓ Il faut avertir l'éditeur ou l'équipe de développement de la vulnérabilité, puis attendre un correctif. Un bulletin de sécurité est ensuite publié.

Attention :

- ✓ Il arrive parfois qu'une vulnérabilité soit publiée sans que l'éditeur n'en soit averti, ou que la vulnérabilité est gardée secrète pour une utilisation malveillante.

De la vulnérabilité à l'exploit :

Conduite à tenir face aux vulnérabilités :

- ✓ Se tenir informé des nouvelles vulnérabilités
- ✓ Appliquer les correctifs
- ✓ Désactiver la fonctionnalité générant la vulnérabilité

Bien comprendre la portée des vulnérabilités et les risques associés

Les exploits : Ce sont des programmes permettant de tester une vulnérabilité, en tentant de l'exploiter. Ils sont écrits par le découvreur de la vulnérabilité ou par des indépendants, en se basant sur les détails fournis dans l'avis initial. L'exploit est ensuite ajouté à un scanner de vulnérabilité pour tester l'efficacité du correctif.

3 Liste des risques de sécurité informatique

Le risque est la probabilité qu'une menace particulière puisse exploiter une vulnérabilité donnée du système.

L'écart entre la menace virtuelle et son niveau de protection correspond au risque, accepté ou résiduel.

3.1 Physiques

Incendie:	Destruction totale ou partielle d'équipements
Dégât des eaux, crues :	Destruction totale ou partielle locaux ou équipements (ex : foudre)
Pollution :	Présence de vapeur, de gaz corrosifs ou toxiques
Accidents majeurs :	Explosion de sites industriels, accident d'avion

3.2 Naturels

Phénomène climatique :	Conditions extrêmes de chaleur et de froid
Phénomène sismique, volcanique :	Zone à risque
Phénomène météorologique :	Tempêtes, ouragans, pluies de grêle

3.3 Rayonnements

Rayonnements électromagnétiques, thermiques :	Radar, antenne radio, rayonnements etc… (micro coupures)

3.4 Compromission des informations et des fonctions

Interception de signaux parasites compromettants :	Possibilité de se connecter aux câblages, tuyauteries etc…
Espionnage à distance / Ecoute passive :	Surveillance de l'activité (câble, réseau…
Vol de supports ou de documents :	Vol de supports magnétiques ou papier
Vol de matériels :	Micro-ordinateurs, modems, etc.

Divulgation interne / externe :	Accidentelle ou intentionnelle (téléphone télécopie, messagerie..)
Informations sans garantie d'origine :	Faux ou contrefaçons (atteinte fiabilité informations)
Piégeage du matériel :	Pour permettre l'interception et la transmission d'informations
Utilisation illicite du matériel :	Pour bénéficier des services rendus par le système
Piégeage du logiciel :	Fonctions cachées (virus, cheval de Troie, trappe, canal caché..)
Abus de droit :	Ex-administrateur réseau qui modifie les caractéristiques d'exploitation
Usurpation de droit :	Usurpation d'identité / substitution (interception//connexion)
Fraude :	Monétaire / Ex : utilisation codes carte bleue
Altération du logiciel :	Action visant à altérer ou détruire les programmes (ex: bombe logique)
Copie frauduleuse du logiciel :	Copies pirate par le personnel
Utilisation de logiciels contrefaits ou copiés sans le savoir	
Altération des données :	Interception avec modification, balayage (numéros d'accès), virus
Atteinte à la disponibilité du personnel :	Maladie ou tout empêchement, volontaire (absentéisme…)

3.5 Défaillance technique

Panne matériel :	Usure, vieillissement, défaut de maintenance, mauvais emploi
Dysfonctionnement matériel :	Dégradations, erreurs de programmation…
Saturation du matériel :	Engorgement, dépassement calcul, stockage, requêtes…
Dysfonctionnement logiciel :	Mauvaise conception, installation, modifications du logiciel

Atteinte à la maintenabilité du SI :	Problèmes fournisseurs, problèmes administratif (séquestre des programmes source)

3.6 Agression Physique, Erreur

Destruction des matériels :	Ex : sabotage des supports de données
Reniement d'actions :	Id répudiation = négation de participation à un échange d'informations
Erreur de saisie :	Ex : données fausses
Erreur d'utilisation :	Manipulation, utilisation matériels, virus…

4 Les types d'attaques sur un réseau

Les informations ou les systèmes d'informations d'une entreprise peuvent subir des dommages de plusieurs façons : certains intentionnels (malveillants), d'autres par accident.
Ces événements seront appelés des « attaques ».

Il existe quatre catégories principales d'attaque :

- L'accès;
- La modification;
- Le déni de service;
- La répudiation.

Les attaques peuvent être réalisées grâce à des moyens techniques ou par ingénierie sociale. L'ingénierie sociale consiste à employer des méthodes non techniques pour obtenir un accès non autorisé.

4.1 Les attaques d'accès

Une attaque d'accès est une tentative d'accès à l'information par une personne non autorisée. Ce type d'attaque concerne la confidentialité de l'information.

4.2 Le sniffing

Cette attaque est utilisée par les pirates informatiques pour obtenir des mots de passe. Grâce à un logiciel appelé renifleur de paquets (sniffer), on peut intercepter toutes les paquets qui circulent sur un réseau même ceux qui ne nous sont pas destinés. Par exemple, lors d'une connexion grâce à « telnet » le mot de passe de l'utilisateur va transiter en clair sur le réseau. Il est aussi possible de savoir à tout moment quelles pages web regardent les personnes connectées au réseau, les sessions ftp en cours, les mails en envoi ou réception. Cette technologie n'est pas forcement illégale car elle permet aussi de détecter des failles sur un système.

4.3 Les chevaux de Troie

Les chevaux de Troie sont des programmes informatiques cachés dans d'autres programmes.
Ce nom vient de la légende grecque de la prise de Troie à l'aide d'un cheval en bois rempli de soldats qui attaquèrent la ville une fois à l'intérieur.
En général, le but d'un cheval de Troie est de créer une porte dérobée (backdoor) pour qu'un pirate informatique puisse ensuite accéder facilement l'ordinateur ou le réseau informatique. Il peut aussi voler des mots de passe, copier des données, exécuter des actions nuisibles.

4.4 Porte dérobée

Lorsqu'un pirate informatique arrive à accéder à un serveur à l'aide d'une des techniques présentées dans cette section, il souhaiterait y retourner sans avoir à tout recommencer. Pour cela, il laisse donc des portes dérobées (backdoor) qui lui permettrons de reprendre facilement le contrôle du système informatique.

Il existe différents types de portes dérobées :

- Création d'un nouveau compte administrateur avec un mot de passe choisi par le pirate.
- Création de compte ftp

- Modification des règles du pare-feu pour qu'il accepte des connections externes.

Dans tous les cas, l'administrateur pert le contrôle total du système informatique. Le pirate peut alors récupérer les données qu'il souhaite, voler des mots de passe ou même détruire des données.

4.5 L'ingénierie sociale

L'ingénierie sociale (social engineering en anglais) n'est pas vraiment une attaque informatique, c'est plutôt une méthode pour obtenir des informations sur un système ou des mots de passe.
Elle consiste surtout à se faire passer pour quelqu'un que l'on n'est pas (en général un des administrateurs du serveur que l'on veut pirater) et de demander des informations personnelles (login, mots de passe, accès, numéros, données…) en inventant un quelconque motif (plantage du réseau, modification de celui-ci…). Elle se fait soit au moyen d'une simple communication téléphonique ou par courriel.

4.6 Le craquage de mots de passe

Le craquage consiste à faire de nombreux essais jusqu'à trouver le bon mot de passe.
Il existe deux grandes méthodes :

- **L'utilisation de dictionnaires** : le mot testé est pris dans une liste prédéfinie contenant les mots de passe les plus courants et aussi des variantes de ceux-ci (à l'envers, avec un chiffre à la fin…). Les dictionnaires actuels contiennent dans les 50 000 mots et sont capables de faire une grande partie des variantes.
- **La méthode brute** : toutes les possibilités sont faites dans l'ordre jusqu'à trouver la bonne solution.

4.7 Les attaques de modification

Une attaque de type « modification » consiste, pour un attaquant à tenter de modifier des informations. Ce type d'attaque est dirigé contre l'intégrité de l'information.

4.8 Virus, vers et chevaux de Troie

Il existe une grande variété de virus. On peut cependant définir un virus comme un programme caché dans un autre qui peut s'exécuter et se reproduire en infectant d'autres programmes ou d'autres ordinateurs.
Les dégâts causés vont du simple programme qui affiche un message à l'écran au programme qui formate le disque dur après s'être multiplié. On ne classe cependant pas les virus d'après leurs dégâts mais selon leur mode de propagation et de multiplication :

- Les vers capables de se propager dans le réseau;
- Les « chevaux de Troie » créant des failles dans un système;
- Les bombes logiques se lançant suite à un événement du système;
- Les canulars envoyés par mail.

4.9 Les attaques par saturation (déni de service)

Les attaques par saturation sont des attaques informatiques qui consiste à envoyer des milliers de messages depuis des dizaines d'ordinateurs, dans le but de submerger les serveurs d'une société, de paralyser pendant plusieurs heures son site Web et d'en bloquer ainsi l'accès aux internautes.
Cette technique de piratage assez simple à réaliser est jugée comme de la pure malveillance.
Elle ne fait que bloquer l'accès aux sites, sans en altérer le contenu.
Il existe différente attaque par saturation :

- Le flooding
- Le TCP-SYN flooding
- Le smurf
- Le débordement de tampon

4.10 Le flooding

Cette attaque consiste à envoyer à une machine de nombreux paquets IP de grosse taille. La machine cible ne pourra donc pas traiter tous les paquets et finira par se déconnecter du réseau.

4.11 Le TCP-SYN flooding

Le TCP-SYN flooding est une variante du flooding qui s'appuie sur une faille du protocole TCP .En effet, on envoie un grand nombre de demande de connexions au serveur (SYN) à partir de plusieurs machines. Le serveur va envoyer un grand nombre de paquet SYN-ACK et attendre en réponse un paquet ACK qui ne viendra jamais. Si on envoie les paquets plus vite que le timeout des « demi-connexion » (connexions autorisées mais non terminé), le serveur sature et finit par se déconnecter.

4.12 Le smurf

Le smurf est une attaque qui s'appuie sur le ping et les serveurs de broadcast . On falsifie d'abord son adresse IP pour se faire passer pour la machine cible. On envoie alors un ping sur un serveur de broadcast. Il le fera suivre à toutes les machines qui sont connectées qui renverront chacune un « pong » au serveur qui fera suivre à la machine cible. Celle-ci sera alors inondée sous les paquets et finira par se déconnecter.

PONG =Echo Reply Without Request" ou "ICMP echo reply attack

4.13 Le débordement de tampon

Cette attaque se base sur une faille du protocole IP. On envoie à la machine cible des données d'une taille supérieure à la capacité d'un paquet. Celui-ci sera alors fractionné pour l'envoi et rassemblé par la machine cible. A ce moment, il y aura débordement des variables internes. Suite à ce débordement, plusieurs cas se présentent : la machine se bloque, redémarre ou ce qui est plus grave, écrit sur le code en mémoire.

4.14 Les attaques de répudiation

La répudiation est une attaque contre la responsabilité. Autrement dit, la répudiation consiste à tenter de donner de fausses informations ou de nier qu'un événement ou une transaction se soient réellement passé.

4.15 Le IP spoofing

Cette attaque consiste à se faire passer pour une autre machine en falsifiant son adresse IP. Elle est en fait assez complexe. Il existe des variantes car on peut spoofer aussi des adresses e-mail, des serveurs DNS ou NFS.

4.16 watering hole ("Trou d'eau")

Pour ce type de menace, l'attaquant infecte un site web, tel qu'un blog ou le site d'une PME, fréquemment visité par la victime ciblée. Lorsque la victime se connecte au site infecté, un dispositif d'attaque ciblée est installé à son insu sur son ordinateur .

5 Liste de mesures à mettre en place

La liste de mesures non exhaustive en vue de réduire ces risques.

5.1 Mesures Physiques

- Protection électrique / régulation électrique (onduleur, …)
- Détection et protection anti incendie
- Système détection eau
- Accès physique restreint / détection d'intrusion
- Température régulée (locaux informatiques)
- Antivol matériel
- Redondance (multiplication machines, cartes, …)

5.2 Mesures Techniques

- Antivirus
- Sauvegarde
- Contrôle des sauvegardes (reprise, redémarrage)
- PROXY + Logiciel administration réseau
- Mots de passe par poste informatique
- Système d'authentification / identification informatique
- Firewall + Routeur filtrant
- VPN (Réseau privé virtuel)
- Cryptage / chiffrement de données
- Plan de sécurité du SI (connexions, modem, …)
- Maintenance (matériel, clim, électrique, accès, …)
- Administration base de données (modification, accès, …)
- Test de sécurité (envoi de données parasites, …)

5.3 Organisation / Plan de sécurité

- Assurance matériel / immatériel / exploitation
- Règles de mise à jour des anti-virus
- Procédures de sauvegarde (nombre, fréquence, stockage, …)
- Définition des responsabilités (restrictions, éthique, …)
- Règles de sécurité informatique (confidentialité, …)
- Centralisation des achats informatiques (licences..)
- Protection des fichiers de base (initialisation, versions, programmes source)
- Règles de gestion des mots de passe (de session, …)
- Règles d'interface informatique / utilisateurs
- Protocole de conception des applications
- Disponibilité personnel informatique / prestataires
- Contrôle des interventions (télémaintenance, sur site, …)
- Solution de secours si indisponibilité du personnel
- Plan et moyens de secours
- Plan et moyens de redémarrage
- Journal des connexions internes et externes (attaques)
- Formation sécurité
- Audits sécurité

6 Introduction à la Sécurité d'un Réseau.

La sécurité est l'ensemble des lois, des règles et pratiques qui régissent la façon dont l'information sensible et les autres ressources sont gérées, protégées et distribuées à l'intérieur d'un système spécifique

Les propriétés principales attendues d'un réseau sont :

- **La disponibilité** : Il s'agit d'assurer que le réseau rende le service pour lequel il a été conçu sans interruption ou déni de services. La disponibilité d'un réseau est généralement assurée par son architecture ou topologie.

- **L'intégrité** : Il s'agit d'empêcher la corruption des données par des fautes accidentelles ou intentionnelles, et à garantir leur mise à jour. L'intégrité est généralement assurée par les protocoles réseaux employés afin de gérer les flux de données, le routage, etc.

- **La confidentialité** : La confidentialité peut être définie comme la prévention de la divulgation non-autorisée de l'information, nous considérons que les données associées aux flux réseaux sont protégées en amont avant de transiter par le réseau.

  L'utilisation d'algorithmes de chiffrement assurera la confidentialité des données.
  En revanche, nous devons absolument considérer l'étanchéité des services réseau, par exemple un VPN doit être isolé des autres VPNs du réseau par défaut, afin de garantir le niveau de confidentialité attendu du service (il s'agit ici de garantir l'isolation logique des trafics réseau).

La sécurité du réseau peut se développer dans les trois directions suivantes :

- **Une politique de sécurité physique** : Elle détaille par exemple les objectifs et règles de sécurité des équipements réseau afin de faire face aux menaces comme le feu, les catastrophes naturelles, etc.,

- **Une politique de sécurité administrative** : Elle détaille par exemple les objectifs et règles de sécurité des procédures de gestion du réseau afin de faire face aux événements de congestion du réseau, etc.,

- **Une politique de sécurité logique** : Elle détaille par exemple les objectifs et règles de sécurité de configuration des accès des équipements réseau afin de faire face aux accès non autorisés, attaques, etc.

7 La Sécurité Physique.

Le premier aspect de la sécurité qui est indépendant du système d'exploitation c'est la sécurité physique. La sécurité physique traite des aspects de la sécurité des équipements informatiques (ordinateurs, Equipements réseau, baie de stockage,..) relatifs à la situation physique de la machine ou de l'environnement où elle opère. La sécurité physique est importante parce qu'elle représente la première barrière sécurisant notre système d'informations contre d'éventuelles attaques ou malveillances

Elle consiste essentiellement à se protéger contre les vols, fuites d'eau, incendies, coupures d'électricité, etc.

Les règles à considérer sont les suivantes :

- Une salle contenant des équipements réseau ne doit pas être vue de l'extérieur afin de ne pas attirer ou susciter des idées de vol ou de vandalisme.

- Une salle d'équipements réseau ne doit jamais être installée au rez-de-chaussée d'un bâtiment afin de ne pas être vulnérable à une inondation.

- Des périmètres de sécurité physique à accès restreint doivent être définis, et équipés de caméras de surveillance.

- Les ressources critiques doivent être placées dans le périmètre le plus sécurisé.

- Toute modification physique d'infrastructure doit être identifiée, reportée et validée.

- Des procédures doivent autoriser et révoquer l'accès aux périmètres de sécurité.

- Le site ne doit pas se trouver pas sur un lieu connu pour des catastrophes naturelles comme la foudre, tremblement de terre, inondation, etc.

- Des équipements de protection contre le feu, l'eau, l'humidité, les pannes de courant, le survoltage, etc., doivent être installés.

- Des procédures de supervision des éléments de protection doivent être mises en place.

8 Périmètre de la Sécurité Physique.

8.1 Sécurité physique des Locaux et Matériels.

Classifications des locaux

Pour une meilleur sécurité il y a lieu d' assurer la séparation des locaux IT, techniques et télécoms , c'est pourquoi il est important d'avoir une classification des locaux suivant les critères suivants:

- **Z0** : Zone où sont localisés les bâtiments. Il s'agit en général du site dans son ensemble.
- **Z1** : Zone d'un bâtiment permettant de recevoir du public (hall, salles de réunions, salles de formation sans matériel informatique, etc.)
- **Z2** : Zone interdite au public en grand nombre et autorisée au personnel ainsi qu'au public isolé ou encadré (bureaux de personnel, salles de formation, salles de réunion interne, salles informatiques hébergeant des informations non sensibles, etc.)
- **Z3** : Zone restreinte au seul personnel habilité (bureaux sensibles)
- **Z4** : Zone dédiée à la protection des infrastructures critiques du système d'information (salle serveur)

Identification des risques.

Les risques clairement identifies et auxquels nous devons prendre des dispositions pour parer aux éventuelles pertes sont les suivants:

- **Le feu**
- **L'eau/ Inondation**
- **L'électricité**
- **La Climatisation**
- **Le Vol**
- **L'Accès non Contrôler**

Salle Serveur

Les salles serveurs doivent être au cœur de l'attention de l'équipe informatique.

Les points suivants sont essentiels et doivent être respectés au plus vite :

- Accès doit être sécuriser (clef, code, etc.)
- La salle serveur doit être aveugle, et ne doit pas posséder de fenêtres non opacifiées et non protégées par grilles ou des barreaux
- la salle des serveurs ne doit pas être installer en sous-sol pour les risques d'inondation et d'accès difficile pour les secours et d'évacuation délicate des fumées.
- La salle serveur doit être à l'abri des conduites d'eau et ne doivent pas être inondables.
- Le nombre de personnes ayant accès à la salle serveur doit être limité (le personnel d'entretien ne doit pas pouvoir rentrer dans ces locaux)
- Le Local doit être sous alarme contre incendie
- Le Local doit être sous alarme contre intrusion
- La salle serveur doit être utilisée à seule fin d'abriter les serveurs, éléments actifs, et autre matériel du système d'information.
- Protection électrique des serveurs vitaux (onduleurs, parafoudres, etc.)
- Climatisation (obtention d'une température adéquate au fonctionnement des serveurs)
- Les portes d'accès des racks doivent être verrouiller
- La signalisation de la salle ne doit pas être affichée.

Locaux Techniques

- L'Accès doit être sécuriser (clef, code, etc.)
- Le Local doit être sous alarme contre incendie
- Le Local soit être sous alarme contre intrusion
- La Protection électrique des équipements actifs (onduleurs, parafoudres, etc.)
- Climatisation (obtention d'une température adéquate au fonctionnement équipements)
- Le Local ne doit pas être installer en sous-sol pour les risques d'inondation et d'accès difficile pour les secours et d'évacuation délicate des fumées
- Les portes d'accès des racks ou coffrets doivent être verrouiller

8.2 Recommandations de Sécurité Physique.

8.2.1 La Localisation.

De la localisation la salle informatique va dépendre une quantité de travaux plus ou moins importantes pour qu'elles soit conforme à l'état de l'art.

- S'assurer que tous les matériels informatiques peuvent être acheminés dans la salle informatique.
- Choisir un local ou il est possible d'acheminer des équipements de 3m de hauteur et de 1000Kg.

- Vérifier les hauteurs de portes de tout le circuit acheminement.
- Vérifier le poids supporter par les Ascenseurs et les montes charges
- le choix du local ne doit pad être inondable (pas de locaux sanitaires au-dessus , pas de canalisation d'eau au dessus ou en dessous, pas de proximité de cours d'eau)
- Le Local de doit pas être situé à proximité d'installation électrique ou radio de forte puissance (les systèmes sont sensibles aux rayonnements magnétiques et électromagnétiques).
- Les équipements actifs du réseau, quand ils sont situés dans des zones accueillant du public, doivent être protégées dans des boîtiers /armoires fermant à clef

8.2.2 La Structure

La construction de la salle informatique doit répondre à des critères de Bases:

- Mise en place d'un faux Plancher (ou plancher technique) de 50 cm utile.
- Le faux Plancher doit résister à 1000 KG au m^2
- Une Chandelle de faux plancher sur 4 doit être reliée à la terre.
- Les Chandelles de faux planchers doivent être fixées au sol par vis et non pas posées ou collées.
- La hauteur utile en ambiance doit être au minium de 3m
- Mise en place d'une galerie technique (chemin de câbles) jouxtant la salle informatique afin d'y mettre en place les servitudes techniques (Climatisation, onduleur, électricité,...)
- Porte à accès contrôlé pour la salle. (contrôle d'accès)
- Mettre en place des cloisons et portes pare-feu
- Dans la mesure du possible les 4 murs, le vrai plancher et le vrai plafond doivent être coupe feu 2 heures vis à vis des locaux adjacents.
- Installer des reports des alarmes sonores (Climatisation, onduleurs, électricité,...) dans un endroit ou se trouve le personnel qualifié.
- Installer un téléphone en salle

8.3 L'Infrastructure Electrique.

8.3.1 L'Alimentation Electrique Générale

L'alimentation électrique est soumise à des normes propre à chaque pays .Le minimum est donc d'effectuer les installations en tenants compte de ces normes.
La puissance nécessaire au fonctionnement de la salle se calcule en faisant la somme des puissances électriques des serveurs, des climatiseurs et de tout autre élément (réseau, etc...).

- Alimenter le local à partir de 2 alimentations principales distinctes.(sous stations électriques par exemples)
- Tenir compte dés l'installation des possibilités d'extension (Ajout d'équipements).

8.3.2 Le Groupe Electrogène.

Le rôle du groupe électrogène est de prendre le relais en cas de coupure d'alimentation électrique générale.

- Il doit être capable d'alimenter l'ensemble des équipements de la salle informatique pendant la durée de réparation de l'alimentation Générale.

- La puissance du groupe électrogène doit être au moins à 2 fois la puissance totale des onduleurs qu'il doit suppléer(Ex:50KVA,150KVA,...)
- Vérifier la cohérence entre la taille du groupe électrogène et celle des onduleurs.
- La taille de réservoir est à évaluer en fonction de l'autonomie désirée(environs 0.25 litres par heure et par KVA).
- Le réservoir du groupe doit permettre une autonomie de 24 heures au minimum
- Penser à remplir le réservoir à chaque fois que des testes de fonctionnements sont opérés.

8.3.3 Les Onduleurs.

Les caractéristiques essentielles de l'onduleur sont:

- La puissance totale utile (KVA)
- La durée d'autonomie en cas de coupure électrique (capacité des batteries)
- Installer deux onduleurs redondant pour parer à toute panne d'onduleur
- Installer les onduleurs dans le local technique et non dans la salle informatique
- Climatiser le local technique
- Déterminer l'autonomie de l'onduleur en tenant compte d'un problème de démarrage du groupe électrogène.
- Tenir compte dés l'installation des possibilités d'extension (Ajout d'équipements)
- Vérifier la cohérence entre la taille du groupe électrogène et celle des onduleurs

8.3.4 Le Câblage Electrique.

- Les tableaux électriques doivent comporter autant de disjoncteurs de connexions électriques nécessaires dans le faux plancher.
- Déterminer le nombre de connexions 16,20 et 32 ampères en fonction de la nature et du nombre d'équipements à installer
- Les câbles électriques partant des tableaux électriques vers la salle informatiques doivent suivre les chemins de câbles réservés.
- Installer les armoires électriques dans le local technique.
- Ne pas mettre les Câbles courant fort et courant faibles dans le même chemin de câble.
- ne pas poser les câbles électriques à même le sol
- Tenir compte dés l'installation des possibilités d'extension (Ajout d'équipements)
- Aucune rallonge électrique ou multiprise ne doit se trouver dans le faux plancher.
- Mettre au moins une mise à la terre tous les 4 chandelles (chandelle de faux plancher)
- Mettre des prises en ambiances permettant la connexion d'équipements volants.

8.4 La Climatisation.

- A fin au les équipements informatiques fonctionnent dans les meilleurs conditions, la température doit être entre 20°C et 22 °C en moyenne et l'humidité doit être de l'ordre de 50%.
- La taille du climatiseur dépend du volume à traiter et du dégagement calorifique des équipements de la salle. Seuls les calculs tenants compte de ces éléments pourront déterminer la nature du climatiseur à installer.
- Considérer dans le calcul de puissance frigorifique les apports externes:
  - luminaires
  - rayonnement des cloisons
  - baies et vitres
  - air neuf.
- Connecter les climatiseurs sur un tableau électrique différent de ceux pour les équipements de la salle
- En cas d'humidité très forts installer un caisson de déshumidification autonome.

8.5 La Protection Incendie.

- Les capteurs doivent être installes tant dans le faux plancher qu'ambiance (plafond)
- installer les systèmes de protection incendie dans le local technique
- Déterminer la nature de l'extinction automatique en fonction de la nature des équipements et en fonctions de la taille de salle informatique.
- Vérifier que le Gaz utilisé est autorisé.
- Prévoir des extincteurs à mains (CO2) en salle informatique et dans les locaux techniques.

8.6 Le Contrôle d'Accès.

L'accès au locaux doit être réglementer en mettent en place des mécanismes de contrôles d'identité :

- Accès par badges à puces
- Tout le monde doit être badgé, et pas seulement les visiteurs
- Reconnaissance biométrique dans la mesure du possible
- Accès en fonction des besoins et non des personnes.
- Accès aux locaux limités aux seules personnes habilitées.
- Garder des traces de tous les accès (positifs ou négatifs)
- Les visiteurs étranger au site doit être accompagner
- Sensibiliser les collaborateurs de l'entreprise aux intrusions (Ils ne doivent pas hésiter à interroger une personne inconnue croisée dans les locaux, afin de connaître l'objet de sa visite.)

8.7 La vidéo Surveillance.

- Les locaux sensibles doivent mises sous vidéosurveillance pour parer à d'éventuels incidents.
- Le système de vidéosurveillance doit être calibré pour répondre de manière pertinente et efficace aux besoins identifiés.
- Affirmer l'obligation de confidentialité qui incombe aux gestionnaires du système.

9 La Sécurité Administrative.

L'exploitation du réseau et de ses services associés doit suivre un ensemble de procédures dites opérationnelles afin d'en assurer l'intégrité et la sécurité à moyen terme. Les règles à considérer sont les suivantes :

- Les procédures opérationnelles doivent être définies et mises à jour.
- Des procédures opérationnelles doivent exister pour la supervision des éléments critiques.
- Des procédures de maintenance préventive doivent exister pour les éléments critiques de telle sorte que toute anomalie soit vérifiée et corrigée.
- Des sauvegardes des informations critiques doivent être effectuées dans un lieu physique distinct de la source. Cela couvre en premier lieu les configurations des équipements.
- Tout problème détecté doit être identifié et résolu.
- Des contre-mesures doivent permettre de vérifier que des problèmes ne restent pas sans solution.
- Tout problème ou incident de sécurité doit être remonté par les procédures opérationnelles aux responsables des domaines visés.
- Les procédures d'incident de sécurité doivent être connues de tout le personnel.

9.1 Compte -Rendu d'alarme.

Ils portent sur les différents types d'alarmes :

- Communications
- Qualité de service
- Traitements
- Equipements

Il est possible de signaler une cause probable pour chaque type, la sévérité perçue, la tendance (alarme plus sévère, moins sévères ou sans changements) .

Causes probables :

Communications :

- perte du signal
- erreur de trame
- erreur de transmission locale
- erreur de transmission distante
- erreur d'établissement de connexion

Qualité de Service :

- Temps de réponse excessif
- Débordement de queue

Traitement :

- capacité de stockage dépassé
- Erreur de version

Environnement:

- incendie-fumées
- humidité excessive
- température excessive

Sévérité perçue

- Clair après prise en compte
- Indéterminée
- Critique
- Majeure
- Mineur
- Attention (Warning)

Informations de seuil

- Valeur Observé
- Seuil de déclenchement de l'alarme
- Niveau de seuil en cas d'hystérésis (est la propriété d'un système qui tend à demeurer dans un certain état quand la cause extérieure qui a produit le changement d'état a cessé)
- Temps d'armement (depuis le dernier réarmement)

9.2 Compte -Rendu d'événements.

Cette fonctionnalité permet de traiter et de rapporter à d'autres systèmes les notifications d'événements.
L'événement notifié est traité localement et/ou rapporté à d'autres systèmes (pour traitements local ou rapport à distance).Ceci est réalisé soit par notification (autre événement) soit par un compte - rendu d'événement.

10 La Sécurité Logique

La sécurité réseau logique porte sur les configurations des équipements réseau. Les configurations détiennent toute l'information permettant de construire le réseau et ses services.
La sécurité réseau logique peut se décliner en un ensemble de règles de sécurité génériques suivantes garantissant la disponibilité et l'intégrité du réseau et de ses services.

Règles de sécurité génériques	Description
Consistance du plan d'adressage	Il s'agit des règles qui garantissent la consistance du plan d'adressage des équipements réseau. De manière générique, il ne doit exister de doublons ni dans le plan d'adressage global du réseau, ni dans le plan d'adressage d'un VPN donné.

Consistance des configurations	Il s'agit des règles qui garantissent la consistance des configurations des équipements réseau. De manière générique, tout élément de configuration défini doit être appliqué, et tout élément de configuration appliqué doit être défini. Ces règles peuvent être complexes comme la vérification de la grammaire associée au langage de configuration.
Consistance des filtrages	Il s'agit des règles qui garantissent la consistance des filtrages utilisés pour contrôler par exemple les flux de données ou de routage. De manière générique, les éléments constituant un filtrage ne doivent être ni redondants, ni contradictoires entre eux. Ces règles peuvent être complexes comme la vérification des règles inutiles.
Routage	Il s'agit des règles de configuration relatives à la protection du routage réseau. Ces règles s'appliquent à la fois au routage interne du réseau ainsi qu'aux interconnexions de routage du réseau avec l'extérieur. Ces règles peuvent être complexes comme la vérification de la topologie du routage interne et externe du réseau, la consistance de la politique de routage, etc.
Service	Il s'agit des règles de configuration relatives à la protection des services du réseau. Ces règles peuvent être complexes comme la vérification des périmètres de sécurité d'un VPN.
Partenaires	Il s'agit des règles de configuration relatives à la protection des interconnexions avec les services réseau d'un partenaire.
Administration	Il s'agit des règles de configuration relatives à la protection des équipements réseau.

11 La Sécurité des Accès Logiques.

La gestion des identités et des accès a pour objectif de mettre en place est un ensemble d'outils et de procédures permettant par des mécanismes de renforcer le contrôle des accès au système d'information, afin de protéger l'intégrité et la confidentialité des données. Et par la nécessité de disposer d'une traçabilité de bout en bout des actions effectuées par chacun.

11.1 Intérêts de la Gestion des Identités et des Accès

La Gestion des Identités et des Accès efficace permet de posséder un référentiel fiable de ses utilisateurs internes et externes.

Elle attribue après validation hiérarchique, fonctionnelle et technique – des droits d'accès en fonction des besoins et du rôle de l'utilisateur dans l'organisation.

Elle s'assure de l'identité de l'utilisateur au moment où il souhaite avoir accès à des données, ou utiliser des applications et systèmes.

Permettant la gestion d'un cycle de vie de l'identité numérique au sein de l'organisation, en ouvrant les accès sur les ressources du système d'information quand cela est nécessaire, et en les supprimant ou modifiant quand l'utilisateur change de poste ou quitte l'entreprise.

11.2 La Gestion des Identités et des Accès

Elle consiste essentiellement à fournir et garantir les points suivants :

Gestion des identités : rationaliser les identités des utilisateurs, auparavant dispersées dans plusieurs annuaires. Des fonctions pour permettre l'identification rapide des personnes au sein de l'organisation.

Authentification forte : contrôle d'accès aux ressources par carte à puce, biométrie, badge radio etc. Gestion des cartes et certificats, réinitialisation de mots de passe.

Authentification unique (single sign-on ou SSO) : lie plusieurs mots de passe et certificats à un seul moyen d'authentification par utilisateur – typiquement un mot de passe ou une carte à puce.

Réduction des risques : la mise en œuvre de l'authentification unique évite le recours à des post-it ou des mots de passe faibles et/ou uniques pour accéder à plusieurs applications. Les mots de passe secondaires n'ont plus à être mémorisés par les utilisateurs, et peuvent ainsi respecter des règles plus strictes (longueur minimum, complexité, fréquence de renouvellement…).

Gestion de politique : définit les droits d'accès en fonction de règles liées au rôle d'une personne dans l'organisation. Prise en compte de contraintes de séparation des tâches.

Circuit d'approbation : conditionne la mise en place des droits d'accès déduits de la politique de sécurité à une validation, généralement hiérarchique.

Audit et rapports : propose une traçabilité des évènements liés aussi bien à l'usage des ressources qu'à l'affectation des droits .Les rapports d'une manière plus large offrent des possibilités de réaliser des audits et d'assurer la conformité à des règles de bonnes pratiques, de règlementation métier, de standards ou de lois.

11.3 La responsabilité de l'Utilisateur

Dès lors que l'identité d'un utilisateur du système détermine ses privilèges et ses droits d'accès à telles ou telles données, il convient que cette identité soit correctement administrée, qu'elle ne puisse pas être usurpée par un tiers, et que son authenticité puisse être vérifiée.

Avant toute chose, les utilisateurs doivent être convaincus du caractère privé de leur identité : cela semble évident, mais de mauvaises habitudes héritées des premiers temps de l'informatique conduisent encore beaucoup de systèmes à être utilisés par plusieurs personnes sous un compte unique dont tout le monde connaît le mot de passe : une telle habitude doit être combattue sans relâche, parce que sur un tel système aucune sécurité n'existe ni ne peut exister. L'interdiction de telles pratiques figure dans une charte informatique.

Tout utilisateur est responsable de son usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à celle de son entité.
L'utilisation de ces ressources doit être rationnelle et honnête afin d'en éviter la saturation ou le détournement à des fins personnelles.

En particulier :

• il doit appliquer les recommandations de sécurité de l'entité à laquelle il appartient

• il doit assurer la protection de ses informations et il est responsable des droits qu'il donne éventuellement à d'autres utilisateurs, il lui appartient de protéger ses données en utilisant les différents moyens de sauvegarde individuels ou mis à sa disposition ;

• il doit signaler toute tentative de violation de son compte et, de façon générale, toute anomalie qu'il peut constater ;
• il doit suivre les règles en vigueur au sein de l'entité pour toute installation de logiciel ;
• il choisit des mots de passe sûrs, gardés secrets et il ne doit en aucun cas les communiquer à des tiers ;

• il s'engage à ne pas mettre à la disposition d'utilisateurs non autorisés un accès aux systèmes ou aux réseaux, à travers des matériels dont il a l'usage ;

• il ne doit pas utiliser ou essayer d'utiliser des comptes autres que le sien, ni tenter de masquer sa véritable identité ;

• il ne doit pas tenter, directement ou indirectement, de lire, modifier, copier ou détruire des données autres que celles qui lui appartiennent en propre ; en particulier, il ne doit pas modifier le ou les fichiers contenant des informations comptables ou d'identification ;

• il ne doit pas quitter son poste de travail ni ceux en libre-service en laissant des ressources ou services accessibles et il doit se déconnecter, sauf avis contraire de l'administrateur du réseau.

12 Le contrôle d'Accès au Réseau.

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder sont autorisés dans le cadre exclusif de l'activité professionnelle des utilisateurs conformément à la législation en vigueur.

L'utilisation des ressources informatiques partagées et la connexion d'un équipement sur le réseau sont en outre soumises à autorisation. Ces autorisations, délivrées par le directeur de l'entité, sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Ces autorisations peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation, même provisoire, de l'activité professionnelle qui l'a justifiée.

L'entité pourra en outre prévoir des restrictions d'accès spécifiques à son organisation : chiffrement d'accès ou d'authentification, filtrage d'accès sécurisé, etc.

12.1 Règles d'utilisation, de sécurité et de bon usage

Tout utilisateur est responsable de son usage des ressources informatiques et du réseau auxquels il a accès. Il a aussi la charge, à son niveau, de contribuer à la sécurité générale et aussi à celle de son entité.

L'utilisateur s'engage à ne pas apporter volontairement de perturbations au bon fonctionnement des systèmes informatiques et des réseaux (internes ou extérieurs à l'institut), que ce soit par des manipulations anormales du matériel, ou par l'introduction de logiciels parasites connus sous le nom générique de virus, chevaux de Troie, bombes logiques.

Tout travail de recherche ou autre risquant de conduire à la violation de la règle définie au paragraphe précédent ne pourra être accompli qu'avec l'autorisation du responsable de l'entité et dans le strict respect des règles qui auront alors été définies.

• il ne doit pas se connecter ou essayer de se connecter sur un serveur autrement que par les dispositions prévues par ce serveur ou sans y être autorisé par les responsables habilités

• il ne doit pas se livrer à des actions mettant sciemment en péril la sécurité ou le bon fonctionnement des serveurs auxquels il accède

• il ne doit pas usurper l'identité d'une autre personne et il ne doit pas intercepter de communications entre tiers

• il ne doit pas utiliser ces services pour proposer ou rendre accessibles aux tiers des données et informations confidentielles ou contraires à la législation en vigueur

• il ne doit pas déposer des documents sur un serveur sauf si celui-ci le permet, ou sans y être autorisé par les responsables habilités

• il doit faire preuve de la plus grande correction à l'égard de ses interlocuteurs dans les échanges électroniques par courrier, forums de discussions.

• il n'émettra pas d'opinions personnelles étrangères à son activité professionnelle susceptibles de porter préjudice à l'institut ou à ses agents
• il doit respecter les lois et notamment celles relatives aux publications à caractère injurieux, raciste, pornographique ou diffamatoire.

12.2 Les Pratiques à ne pas faires

- Tout Autoriser Par Défaut
  (il faut faire le contraire par exemple au niveau d'un pare-feu tout interdire)

- Prétendre dresser la liste des menaces
  (Il faut au contraire dresser la liste de tous les logiciels utiles, d'usage légitime dans le SI de l'entreprise, et interdire tous les autres en vertu de la règle précédente.)
- Tester par intrusion, puis corriger
  La mise en pratique de cette idée consiste à détecter les failles du système à protéger en perpétrant une intrusion, en d'autres termes, à attaquer son système de protection, pare-feu, antivirus ou autre, puis à obturer les brèches que l'on aura détectées.
  (si vous l'avez fait c'est des pirates l'ont déjà fait avant vous)

  la seule façon d'obtenir un système sûr, c'est qu'il le soit dès la conception, et c'est possible

- Ne pas jouer au Pirates
  Ne pas essayer d'imiter les autres au risque de compromettre sa propre sécurité

- Compter sur l'éducation des utilisateur
  Attendre que les utilisateurs aient été victimes d'un incident de sécurité et d'attaques réussies, et ensuite seulement les corriger (éduquer).

  Si votre politique de sécurité repose sur l'éducation des utilisateurs, alors elle est vouée à l'échec.

  Dans ce cas mieux vaut donc configurer le système de sorte que :

  1. les choses dangereuses ne parviennent pas aux utilisateurs ;
  2. lorsque certaines choses dangereuses passent à travers les mailles du filet (il y en aura), les conséquences en seront limitées, détectées puis contrôlées.

- l'action vaut mieux que l'inaction
  (Adopter avant tout le monde les plus récentes technologies s'expose davantage à des incidents de sécurité que l'administrateur prudent qui attend deux ans la stabilisation du système et les retours d'expérience avant de l'implanter)

  Il est souvent plus facile de ne pas faire quelque chose d'idiot que de faire quelque chose d'intelligent

- Penser que nous ne sommes pas une cible intéressante

- En déployant notre pare-feu préféré nous serons protégés
  Non, le système ou le pare-feu qui protège, c'est celui pour lequel il y a sur le site un ingénieur compétent, qui le connaît bien et qui consacre beaucoup de son temps à s'en occuper ;

- Pas besoin de pare-feu, notre système est sûr
  Non, même avec un système sûr, sans pare-feu toute application réseau est une cible facile

- Pas besoin de sécuriser le système, nous avons un bon pare-feu
  Non, le trafic légitime qui franchit le pare-feu comporte des risques ;

- Démarrons la production tout de suite, nous sécuriserons plus tard » :
  Non, ce ne sera jamais fait, et si cela doit l'être, cela prendra beaucoup plus de temps et de travail que de l'avoir fait au départ
- nous ne pouvons pas prévoir les problèmes occasionnels
  si, vous pouvez; prendriez-vous l'avion si les compagnies aériennes raisonnaient ainsi ?

13 La Sauvegardes des Données.

La sauvegarde (backup en anglais) est l'opération qui consiste à mettre en sécurité les données contenues dans un système informatique. Par extension et par emprunt à l'anglais (to save), ce mot s'applique à tout enregistrement d'information sur un support permanent (par ex. l'écriture sur disque dur d'informations en mémoire vive). Dans ce sens, il est synonyme de « stockage d'information ». Mais le sens premier se rapproche de celui d'archivage, de conservation.

13.1 Déterminer l'information à sauvegarder

Dans la majorité des cas l'information à sauvegarder se rapporte sur :

• Des éléments nécessaires
• Les fichiers de configuration
• Les bases de données (BD)
• Les paramètres importants
• La configuration système
• L'installation d'un logiciel ou d'un outils
• La configuration réseaux

Finalité :

Les copies de sûreté sont utiles principalement à deux choses :

• La première et la plus évidente est de permettre de restaurer un système informatique dans un état de fonctionnement suite à un incident (perte d'un support de stockage tel que disque dur, bande magnétique, etc., ou de tout ou partie des données qu'il contient).

• La seconde, incluse dans la première mais certainement la plus courante, est de faciliter la restauration d'une partie d'un système informatique (un fichier, un groupe de fichiers, un système d'exploitation, une donnée dans un fichier, etc.) suite à une suppression accidentelle ou à une modification non désirée.

La technique la plus fréquente est la recopie des données sur un support indépendant du système initial (ordinateur local, serveur, etc.).

L'opération inverse qui consiste à réutiliser des données sauvegardées s'appelle une restauration. On parle de « stockage » pour les données sauvegardées en attente d'une éventuelle restauration.

Critères de choix :
Le choix d'une technique de sauvegarde se fera en prenant en compte :

• la capacité de stockage du support (le volume d'information)
• la vitesse de sauvegarde,
• la fiabilité du support (notamment après une longue période de stockage),
• la simplicité de classement,
• la facilité à restaurer les données,
• et bien sûr le coût de l'ensemble.

Intervient également la possibilité de sélectionner les données à sauvegarder. Enfin pour les grands systèmes de sauvegarde, il faut tenir compte de critères physiques : volume physique des supports de stockage, poids, sensibilité à la température, à l'humidité, à la poussière, à la lumière.

13.2 Médias de sauvegarde et d'archivage :

Revenons tous d'abord sur la différence entre la sauvegarde et l'archivage. La sauvegarde est un processus permettant de récupérer les données après un incident tandis que l'archivage correspond au déplacement des données du disque dur vers un autre support qui doit permettre l'utilisation de ces données.

Il y a différents média de sauvegarde :
• Disquettes (en disparition pour les formats d'un 1 Mo)
• Bandes QIC à l'aide de streamer, DAT
• Jazz (1 Go) ou Zip (100 Mo)
• Disque dur amovible.
• CD-ROM

De plus, pour la sauvegarde on utilise souvent des algorithmes de compression qui permettent de diminuer la taille prise par les fichiers. Ce gain varie évidemment en fonction des données sauvegardées : textes, images, programmes. La majorité des logiciels de sauvegarde propose ces méthodes de compression ainsi que des méthodes de cryptage pour Éviter que n'importe qui ayant accès à ces bandes puisse reconstruire les fichiers. Mais compression et cryptage peuvent aussi être matérielles c'est-à-dire que le périphérique de sauvegarde décharge le serveur de ces opérations. Un autre point important du logiciel de sauvegarde est sa capacité à détecter les erreurs sur le support de sauvegarde.

Une fois la sauvegarde faite, il ne faut pas conserver ces données prés du serveur car, en cas d'incendie ou tout autre problème physique, on perdra tout, il faut donc conserver ces sauvegardes dans un autre bâtiment dans un coffre ignifugé.

13.3 Stratégies de sauvegarde :

On distingue la sauvegarde sur micro-ordinateur de la sauvegarde sur gros système. L'une et l'autre s'adressent à la même nature d'information (la donnée informatique) et ont le même objectif (protéger l'information et permettre de la retrouver si elle était perdue), mais les méthodes de sauvegarde différente pour plusieurs raisons :

Les données sur micro-ordinateur sont réputées moins importantes que les données gérées sur des systèmes volumineux ; les utilisateurs de micro-ordinateurs sont moins sensibilisés au risque de perte de données que les professionnels de l'informatique ; ils ont également moins de formation sur les techniques de sauvegarde ; les moyens techniques sont moins développés sur micro-informatique

que sur gros systèmes, même si des progrès importants ont été réalisés ces dernières années (chute du rapport coût/volume des supports de sauvegarde, simplification des interfaces de sauvegarde, sauvegarde sans intervention de l'utilisateur, etc.)

De fait en micro-informatique, contrairement aux gros systèmes, le "backup" reste marginal dans la stratégie d'utilisation des ordinateurs. Cependant les entreprises, en généralisant l'usage des micro-ordinateurs et du partage des ressources en réseau, ont ressenti un besoin de sécurité qui a favorisé le développement d'outils de sauvegarde sur micro-ordinateurs, lesquels gagnent petit à petit le monde de la micro-informatique personnelle.

Sauvegarde sur gros système :

La sauvegarde s'inscrit dans une démarche plus globale qui consiste à assurer la continuité d'activité d'un système informatique ou, en cas de défaillance, son redémarrage le plus vite possible. Cette démarche est souvent formalisée dans un document qui peut porter des noms divers, par exemple le "PRA" (plan de reprise d'activité) ou le "PS" (plan de secours), et qui fait appel soit à des automatismes (ex. donner l'alerte en cas de coupure de courant ou de perte d'accès à une unité de stockage) soit à des gestes manuels (ex. remplacer des bandes magnétiques défectueuses). La tendance est à l'automatisation, réputée plus sûre dans les situations d'urgence que les opérations manuelles.

En terme de support, les gros systèmes ont depuis toujours recherché des supports à grande capacité de stockage. La bande magnétique a longtemps été le principal vecteur, du fait de sa grande capacité, de son coût faible (par rapport aux autres supports), de sa capacité de réutilisation et de sa relative stabilité au temps et à l'usure. Puis sont venus les cartouches numériques (bandes magnétiques intégrées dans un boîtier plastique type DAT, DLT), les disques durs et plus récemment les médias optiques, réinscriptibles ou non, tels que les CD-R, DVD-R ou formats similaires.

13.4 Modes de sauvegarde :

Le mode de sauvegarde détermine la façon dont la sauvegarde a lieu en fonction des données à sauvegarder. Il existe deux méthodes pour sauvegarder les données :

• Sauvegardes en ligne (A Chaux): les sauvegardes s'effectuent pendant que les données restent accessibles à tous les utilisateurs.

• Sauvegardes hors ligne (A Froid) : les sauvegardes concernent les données qui sont d'abord mises hors de portée des utilisateurs.

Sauvegardes en ligne (A Chaux):

Les sauvegardes en ligne ont lieu pendant que le système est en ligne. C'est la stratégie de l'interruption la plus courte. Ce type de sauvegarde est généralement utilisé pour les applications devant être disponibles 24 heures/24, telles que Microsoft Exchange Server et Microsoft SQL Server, les deux prenant en charge les sauvegardes en ligne.

Avantages :

Parmi les avantages des sauvegardes en ligne, on retient :

• Pas d'interruption de service :

Les applications et les données restent entièrement accessibles aux utilisateurs pendant le processus de sauvegarde.

La sauvegarde hors des heures de travail n'est plus nécessaire.

Les sauvegardes en ligne peuvent être programmées pendant les heures normales de bureau.

• Sauvegarde partielle ou totale :

Les sauvegardes peuvent être partielles ou totales.

Inconvénients :

Parmi les inconvénients des sauvegardes en ligne, on retient :

- Performances du serveur :

  Au cours du processus de sauvegarde, il est possible que les performances des serveurs de production se dégradent.

- Fichiers ouverts

  Si certaines applications sont actives pendant le processus de sauvegarde, il est possible que les fichiers de données ouverts ne soient pas sauvegardés.

Sauvegardes hors ligne (A Froid) :

Les sauvegardes hors ligne sont effectuées en mettant hors ligne le système et les services. Vous pouvez les utiliser si vous avez besoin d'un instantané du système ou si l'application ne prend pas en charge les sauvegardes en ligne.

Avantages :

Parmi les avantages des sauvegardes hors ligne, on retient :

- Sauvegarde partielle ou totale :
  Avec les sauvegardes hors ligne, vous pouvez choisir entre une sauvegarde partielle ou totale.
- Performances :
  Les sauvegardes hors ligne offrent de meilleures performances de sauvegarde car le serveur peut être dédié à la tâche de sauvegarde.
- Sauvegarde de tous les fichiers

Toutes les données sont sauvegardées dans la mesure où aucune application n'est en cours d'exécution et donc qu'aucun fichier n'est ouvert pendant le processus de sauvegarde.

Inconvénient :

- Interruption du service :

L'inconvénient des sauvegardes hors ligne est que les données ne sont pas accessibles à l'utilisateur pendant l'exécution du processus de sauvegarde.

<u>Les points importants à retenir</u>

- Effectuer une sauvegarde complète des applications logicielles et vérifier qu'elle fonctionne.
  Elle doit être séparée physiquement du système informatique et placer dans un local sécurisé.
- Déterminer les informations à protéger:

- Effectuer une sauvegarde de ces données sur un outil adapté et vérifier que le support n'est pas saturé. Etre attentif à la durée de conservation des sauvegardes.
- Avoir plusieurs supports de sauvegarde, et en fonction de l'activité effectuer une sauvegarde quotidienne en changeant régulièrement de support.
- Ne pas laisser le support de sauvegarde dans le poste de travail ou à côté, il ne doit pas être à la portée du premier venu.
- Centraliser toutes les données sur un même poste pour permettre une sauvegarde généralisée.
- Regrouper les données confidentielles sur un poste isolé du réseau avec un disque dur extractible.
- Externaliser les sauvegardes ou les placer dans un local sécurisé (coffre-fort ignifugé).

14 Que faire en cas d'incident

Nous essayons de répondre aux questions les plus couramment posées.

Ces consignes s'adressent aux administrateurs systèmes et réseaux et aux chargés de SSI de l'unité. Elles supposent que préalablement des procédures internes aient été définies permettant l'information de ces responsables dès la découverte de l'incident.

Caractériser l'incident :

- **Nature** : s'agit-il bien d'un incident touchant directement ou indirectement la SSI ?
- **Type** : compromission de serveur, défiguration de site web, compromission de fichiers sensibles, phishing, mise en cause ou menaces par voie informatique qui doivent être considérées comme relevant d'un incident SSI,...

Le vol de matériel informatique ou supports de données doit être considéré comme relevant d'un incident SSI. Il fait l'objet de consignes spécifiques.

Démarche et recommandations techniques:

- Avertir le chargé de la SSI et le directeur d'unité.
- Supprimer l'accès au système depuis l'extérieur et faire une sauvegarde du système dans son état pour garder des traces.
- Remplir la fiche ou rapport "suivi d'incident"
- Informer en concertation avec le directeur les responsables hiérarchiques
- Faire une première évaluation des dégâts. En particulier, examiner les traces et tous les répertoires pour déterminer le type d'intrusion et quels sont les fichiers compromis et/ou ceux qui ont été ajoutés
- Examiner toutes les autres machines pouvant être compromises.
- Changer tous les mots de passe
- Réinstaller la machine compromise en ayant soin d'avoir corrigé la/les failles de sécurité.
- Faire une sauvegarde et une empreinte du système.
- Réinstaller les comptes utilisateurs.
- Reconnecter la machine au réseau**.**

Veillez à ce que l'information ait bien été reçue par:

- **La hiérarchie organique** : direction de l'unité
- **La chaîne fonctionnelle** SSI de rattachement principale de l'unité ;
- **Les autorités compétentes,** selon la gravité de l'incident et la sensibilité de l'unité

Apprécier l'opportunité de déposer plainte et déterminer "par qui" et "auprès de qui" la plainte doit être déposée

15 Plan de continuité d'activité

Les plans de reprise d'activité doivent être élaborés en suivant une méthodologie de projet rigoureuse car l'existence même de l'entreprise peut être ébranlé.

Objectif :

- Assurer le redémarrage des applications et processus clés de l'entreprise, même en mode dégradé, afin qu'elle poursuive son activité.
- Prévenir les risques majeurs (tels un incendie ou une inondation).
- Assurer le basculement de tout ou partie du système d'information sur un site distant préalablement défini et équipé
- Limiter le temps d'indisponibilité des applications et services
- Réduire les pertes de données.

Identification:

- Quels sont mes services vitaux ?
- Quels sont les processus critiques mis en œuvre dans ces services ?
- Quels flux sont en jeux ?
- Quelles sont les ressources informatiques critiques utilisées par mes processus vitaux ?

Périmètre:

Concerne tous les moyens techniques et humains devant être activés pour assurer le Plan de Continuité d' Activité.

- Hommes
- Systèmes
- Stockage des données
- Réseaux
- Postes de travail
- Logiciels de base
- Applications
- Locaux techniques
- Continuité d'énergie et de froid

Approche: réaliser en "strates"

On doit réfléchir à chaque système et comment assurer ça disponibilité**.**

- Accès
- Réseau
- systèmes et OS
- Applications
- Données (tous types)
- Sauvegardes et Archivage
- Support de transmission (Fibre optique , paire torsadé , etc.)

Options Possibles:

- Accès (Renforcement des liaisons de secours)
- Réseau (Secours sur un autre site)
- systèmes et OS (Physique ou virtuel)
- Applications (Actif/Actif ou Actif/Passif)
- Données (tous types) (Déporté sur Baie et/ou Réplication Asynchrone)
- Sauvegardes et Archivage (Master/Slave) Réplication déporté.
- Support de transmission (Fibre optique , paire torsadé , etc.) Prévoir des Maillages avec des chemins différents

L'idéal: Prévoir

- Salle blanche, un lieu vide mais susceptible d'accueillir par ses infrastructures l'installation d'une solution de reprise d'activité,
- Back'up Mutualisé : Lieu ou des infrastructures techniques sont préexistantes et susceptibles d'assurer la réalisation du plan de continuité mais ce lieu n'est pas exclusif et peut servir à d'autres organisations dans le même but.
- Back'up dédié, Un site équipé en tout point de la même infrastructure hard soft et réseau et dédié à cette fonction pour l'organisation.
- Réplications asynchrones ou journalisation distante : prévoit en plus le transfert au fil de l'eau d'eau des journaux des transactions afin d'assurer une reprise de l'activité dans des délais de l'ordre de quelques heures seulement.
- Réplications synchrones ou Mirroring : Sites distants avec des données recopiées en temps réel de part et d'autre permettant des redémarrages en cas d'incidents dans des délais de l'ordre de quelques minutes voire instantanément si une architecture à redondance totale est prévue.

Technologies Disponibles.

Solutions haute-disponibilité

- Cluster système
- Cluster applicatif
- Cluster d'équipements réseaux

Architecture sécurisée de réseaux multi-sites pour le transport et le stockage de données

- Design d'architecture de réseaux SAN Fibre Channel et iSCSI
- Solutions d'interconnexion SAN longue distante : FC/IP, FC-FC, xWDM, partenariats opérateurs
- Design d'architecture de réseaux LAN et WAN inter sites, VPN SSL, MPLS, etc.

Architecture sécurisée de stockage sur disques

- Solution de réplication du stockage sur disques SAN (Fibre Channel / iSCSI) et NAS
- Solution de virtualisation de ressources de stockage hétérogènes
- Solution de stockage répartie de type MetroCluster
- Solution de réplication et de duplication de base de données

Sécurisation et gestion du cycle des données

- Politique de sauvegarde, de restauration et d'externalisation de vos données (multi supports)
- Gestion des classes de stockage et archivage informatique

15.1 Organisation à mettre en Place.

Pour assure un bon plan de continuité de d'activité , il faut s'assurer qu'une bonne organisation est mise en place pour assurer le pilotage du plan de secours..

Propositions d'organisation.

On distingue les premiers intervenants chargés d'appliquer les consignes et de donner l'alerte selon la procédure d'escalade définie.

On identifiera les intervenants chargés de la résolution du sinistre :

- La structure de crise :
    - Comité de crise
    - Cellule de coordination
- Les équipes d'intervention
- Les services utilisateurs

Le **comité de crise** se compose généralement du Responsable du Plan de Secours et des directions suivantes : Direction Générale, Principales Directions Utilisatrices, Services Généraux, Ressources Humaines, DSI, Communication. Son rôle est de juger de l'opportunité de déclencher le Plan de Secours.

La **cellule de coordination** est chargée du pilotage des opérations de secours. Elle se compose du Responsable du Plan de Secours Informatique et des personnes chargées de la coordination des opérations informatiques et logistiques.

Les équipes d'intervention réalisent les tâches de secours. Elle peuvent comporter des acteurs externes à l'entreprise (fournisseurs d'énergie, opérateur de téléphonie, fournisseur d'accès Internet…). Un « annuaire du plan de secours » devra donc être tenu à jour avec l'ensemble des coordonnées des intervenants internes et externes.

Les **services utilisateurs** prennent en charge leur propre plan de reprise d'activité, notamment : les tâches d'attente du secours, l'organisation du redémarrage, la mise en place des procédures de contournement et l'organisation de travaux exceptionnels.
Il est indispensable que ces services disposent en toute circonstance des compétences humaines connaissant les procédures à suivre dans le contexte de secours.

Le **responsable du plan de secours**, a pour mission les tâches suivantes :

- Effectuer, suivre et gérer les tests du plan et les modifications qui en découlent
- Engager et suivre le processus d'actualisation
- Maintenir, sécuriser et diffuser le plan de secours

Afin de lui permettre de réaliser sa mission, il devra être informé de l'émergence de nouveaux risques, des évolutions techniques et structurelles ainsi que des nouveaux projets.

15.2 Documentations.

La documentation est un élément essentiel du plan de secours. Généralement, volumineuse et très évolutive, elle contient généralement des informations confidentielles directement liées à la stratégie de l'entreprise.

La documentation a 4 objectifs principaux : communiquer, mettre en œuvre, gérer et contrôler.

Documents de communication

Les documents de communication sur le plan de secours doivent permettre aux différents intervenants et responsables d'avoir une bonne vue d'ensemble des solutions prévues.

Ils contiennent généralement :

- un rappel des objectifs
- une description générale des dispositifs
- une description générale de la cellule de crise
- les principes d'alertes
- un rappel des risques résiduels

Documents de mise en œuvre

Destinés aux personnes ayant la responsabilité des différents dispositifs du plan de secours, ce documents contiennent les éléments utiles à la mise en œuvre du plan : procédures, documentation technique, éléments de synchronisation, contrats, …

A minima, on recensera les documents suivants :

- l'annuaire du plan de secours
- la description de la stratégie de secours pour chaque risque identifié
- le planning des phases de reprises
- les fiches des tâches à réaliser
- la feuille de route de chaque acteur du plan
- l'ensemble des annexes utiles

Documents de gestion

Ces documents ont pour objet de permettre la maintenance du plan de secours. Ce sont généralement les documents ayant permis son élaboration : tableaux d'analyse des ressources, listes de diffusion, …
On y intègre également l'historique des résultats de tests et les plans d'ajustement consécutifs.

Documents de contrôle

Ces documents sont les tableaux de bord du plan de secours :

- planning des tests
- comptes rendus détaillés des tests
- indicateurs de qualité des dispositifs et du plan
- évaluation des risques résiduels

15.3 Maintenance du Plan

Plusieurs fois par an, le comité plan de secours doit être réuni afin d'évaluer les nouveaux risques et de proposer le plan d'action correspondant. Ce plan d'action concerne :

- la mise en œuvre des moyens
- l'actualisation des documents
- l'évolution éventuelle des contrats de prestation extérieurs
- les tests des nouveaux secours

15.4 Plan de Test

Le plan de secours doit être validé par un plan de test.

On distingue 3 catégories de tests :

- les **tests techniques unitaires** (1 fois par trimestre) visant à vérifier un élément de secours
- les **tests d'intégration** (1 à 2 fois par an) afin de vérifier la compatibilité des différents éléments de secours, la synchronisation des opérations techniques et la charge des équipes
- les **tests en vraie grandeur** (1 à 2 fois par an) ayant les mêmes caractéristiques que les tests d'intégration avec comme caractéristique supplémentaire un test de réactivité des équipes et une vérification du bon fonctionnement par un travail effectif d'utilisateurs dans des conditions proches d'une situation de crise.

Pour chaque test, les opérations suivantes sont réalisées :

- formalisation des objectifs visés
- description du scénario de test
- préparation du test
- désignation d'un ou plusieurs observateurs
- rédaction d'un compte rendu de test et d'un bilan permettant de prononcer la validation totale ou partielle du plan de secours

16 Mise en Place d'une Politique de sécurité

16.1 Introduction

La sûreté de fonctionnement d'un système informatique ou réseau est la propriété qui permet à ses utilisateurs de placer une confiance justifiée dans les services que ce système lui délivre.

Les notions relatives à la sûreté de fonctionnement peuvent être réparties en trois classes:

- **Les entraves** : elles correspondent aux événements indésirables comme les fautes, les défaillances, les attaques, etc. qui entravent à la sûreté de fonctionnement.
- **Les moyens** : Ils correspondent aux méthodes et techniques comme la prévention des fautes, l'élimination des fautes, etc. permettant d'assurer un service conforme à la fonction attendue.
- **Les attributs** : Ils correspondent aux propriétés attendues d'un système comme la disponibilité, l'intégrité, la confidentialité, etc. permettant de définir les fonctions attendues d'un service.

La politique de sécurité d'un réseau se fonde avant tout sur une analyse des risques décrivant les ressources critiques du réseau, ses vulnérabilités, les probabilités d'occurrence des menaces sur ces ressources vitales, ainsi que leurs conséquences.

À partir de cette politique de sécurité, une architecture, des outils et des procédures sont définis et déployés afin de protéger les ressources critiques et de répondre aux objectifs de sécurité.

Les mesures de sécurité à mettre place peuvent être d'ordre divers, demander des ressources plus ou moins importantes et être implémentées dans des délais plus ou moins réalistes.

16.2 Les recommandations générales

Afin d'éviter un certain nombre d'écueils classiques, une politique de sécurité réseau doit respecter un ensemble de principes. Ces principes permettent notamment de bien cerner les enjeux de la rédaction d'un document de politique de sécurité, qui n'est pas un document comme les autres.

Un document de politique de sécurité peut être écrit de plusieurs manières, allant d'un texte unique à un ensemble de politiques de sécurité. Le choix d'écrire un ou plusieurs documents est le plus souvent dicté par la taille du réseau.
Plus le réseau est important, plus il est intéressant de créer des documents séparés, chaque niveau faisant référence au niveau supérieur.

Une **politique** de sécurité est **l'expression du besoin** de sécurité. La **procédure**, ou

recommandation technique, est l'implémentation du besoin. Il est donc impératif de distinguer les deux. Lorsque certains produits pare-feu présentent les règles de filtrage comme une politique de sécurité, c'est le concept même de politique de sécurité qui est dévoyé. **L'objectif d'une politique** de sécurité est **d'énoncer des résultats attendus**, et **non les moyens par lesquels les obtenir**.

Les principes énoncés par une politique de sécurité assurent à cette dernière une pérennité beaucoup plus longue que les procédures de sécurité, qui sont appelées à être modifiées fréquemment pour tenir compte des avancées technologiques, des modifications d'architecture, etc.

On peut énoncer les principes suivants :

Le principe de propriété : Le principe de propriété exige qu'une politique de sécurité décrive, pour chaque ressource, quels en sont les propriétaires.
On doit entendre par propriété, non pas l'aspect légal de la propriété d'un bien, mais son aspect fonctionnel, qui consiste à en assurer la pérennité et la protection. Les propriétaires d'une ressource en ont la responsabilité et dictent les règles d'accès à cette ressource. Un schéma classique établit une distinction entre le propriétaire, l'administrateur et l'utilisateur d'une ressource. Le propriétaire définit les règles d'utilisation de ses ressources et les donne à l'administrateur, lequel a pour rôle de les appliquer aux demandes d'un utilisateur. En cas de problème, l'administrateur demande au propriétaire une dérogation aux droits d'accès. L'utilisateur n'est jamais en contact direct avec le propriétaire. Ce mode de fonctionnement garantit une certaine indépendance de l'administrateur face à l'utilisateur.

L'autorité : La direction générale a autorité sur toutes les ressources du réseau. Elle délègue généralement cette autorité aux responsables de départements, qui peuvent à leur tour mandater un groupe au sein de leur département. Dans tous les cas, l'équipe sécurité, mandatée par la direction générale, dispose de l'autorité de vérifier l'application de la politique de sécurité sur toutes les ressources du réseau. Un comité de sécurité, constitué des responsables du réseau, doit être constitué afin de définir la stratégie sécurité du réseau et de trancher les problèmes de sécurité remontés par l'équipe sécurité ou d'autres départements.

L'universalité : Le principe d'universalité veut qu'une politique de sécurité dicte des règles qui doivent être non seulement validées, quels que soient les aspects techniques mis en jeu, mais aussi appliquées. L'idée sous- jacente est que la conception initiale d'une politique de sécurité se détache au maximum des aspects technologiques et énonce des règles et principes. Seuls les guides, recommandations ou procédures impliquent des aspects techniques.

L'orthogonalité : Le principe d'orthogonalité précise qu'une politique de sécurité peut être découpée en sous-parties distinctes, sous la condition que ces sous-parties forment un ensemble cohérent. L'idée sous-jacente est que la conception initiale d'une politique de sécurité et de ses domaines d'application doit être essentielle et fondamentale, de sorte à

éviter une évolution inconsistante de la politique de sécurité, de ses guides et de ses recommandations.

La simplicité : Une politique de sécurité est simple dans sa structure et claire dans les règles qu'elle énonce. Toute mauvaise compréhension d'une règle de la politique de sécurité conduit à ce qu'elle ne soit pas appliquée ou, pire, qu'elle le soit mal.

L'auditabilité : Une politique de sécurité est auditable. Cela demande que les règles qu'elle énonce puissent être vérifiées dans les faits. Bien qu'il soit difficile de mesurer toute chose, la politique de sécurité est écrite dans cet objectif. L'idée sous-jacente est qu'une politique de sécurité constitue le référentiel ou la pierre angulaire de tout audit ou contrôle de sécurité. Les règles qu'elle énonce doivent pour cela être claires, précises et mesurables.

La hiérarchie : Une politique de sécurité est structurée en une politique de sécurité de haut niveau, qui englobe les politiques de sécurité couvrant des domaines précis. Ces mêmes politiques de sécurité pointent sur des procédures qui détaillent des aspects techniques du domaine visé. L'idée sous-jacente est qu'une politique de sécurité doit être structurée en sous-politiques de sécurité, dans une approche allant du plus général au plus spécifique. Il est admis que deux à trois niveaux de politiques de sécurité conviennent dans la plupart des cas. Il convient toutefois de prendre garde au piège de l'arborescence des politiques de sécurité, qui pourrait contredire les principes de simplicité et d'orthogonalité.

L'approbation : Une politique de sécurité est approuvée par la direction générale, et ce de manière officielle. De plus, la direction générale et les ressources humaines s'engagent à réprimer toute violation de la politique de sécurité qui pourrait mettre en péril la survie du réseau. Les cadres juridique et réglementaire couvrant la politique de sécurité et les actes de malveillance doivent être connus de tout le personnel du réseau.

Une politique de sécurité est moins touchée par l'évolution technologique, car elle décrit des besoins et non des moyens. Malgré tout, une politique de sécurité doit être revue régulièrement afin de tenir compte des modifications organisationnelles.

Enfin, une politique de sécurité est réaliste et tient compte à la fois des contraintes du réseau et des coûts générés par la sécurité comparés aux gains de sécurité engendrés.

17 Historique et Evolutions des Normes en matière de sécurité de l'information

Au cours des vingt dernières années les normes liées à la sécurité de l'information ont évolué ou ont été remplacées. Ces changements rendent difficile une bonne compréhension du sujet. Un rappel historique de l'évolution de ces normes permet de clarifier la situation normative en matière de sécurité de l'information.

Au début des années 90, de grandes entreprises britanniques se concertent pour établir des mesures visant à sécuriser leurs échanges commerciaux en ligne. Le résultat de cette collaboration servit de référence en la matière pour d'autres entreprises qui souhaitaient mettre en œuvre ces mesures. Cette initiative privée fut appuyée par le Département des Transports et de l'Industrie britannique qui supervisa la rédaction au format du BSI, d'une première version de projet de norme de gestion de la sécurité de l'information.

En 1991, un projet de «best practices» code de bonnes pratiques, préconise la formalisation d'une politique de sécurité de l'information. Cette politique de sécurité doit intégrer au minimum huit points «stratégique et opérationnel6» ainsi qu'une mise à jour régulière de la politique.

En 1995, le BSI publie la norme BS7799 qui intègre dix chapitres réunissant plus de 100 mesures détaillées de sécurité de l'information, potentiellement applicables selon l'organisme concerné.

En 1998, la norme BS7799 change de numérotation et devient la norme BS7799-1. Elle est complétée par la norme BS7799-2 qui précise les exigences auxquelles doit répondre un organisme pour mettre en place une politique de sécurité de l'information. Cette nouvelle norme est fondée sur une approche de la maîtrise des risques et sur le principe du management de la sécurité de l'information.

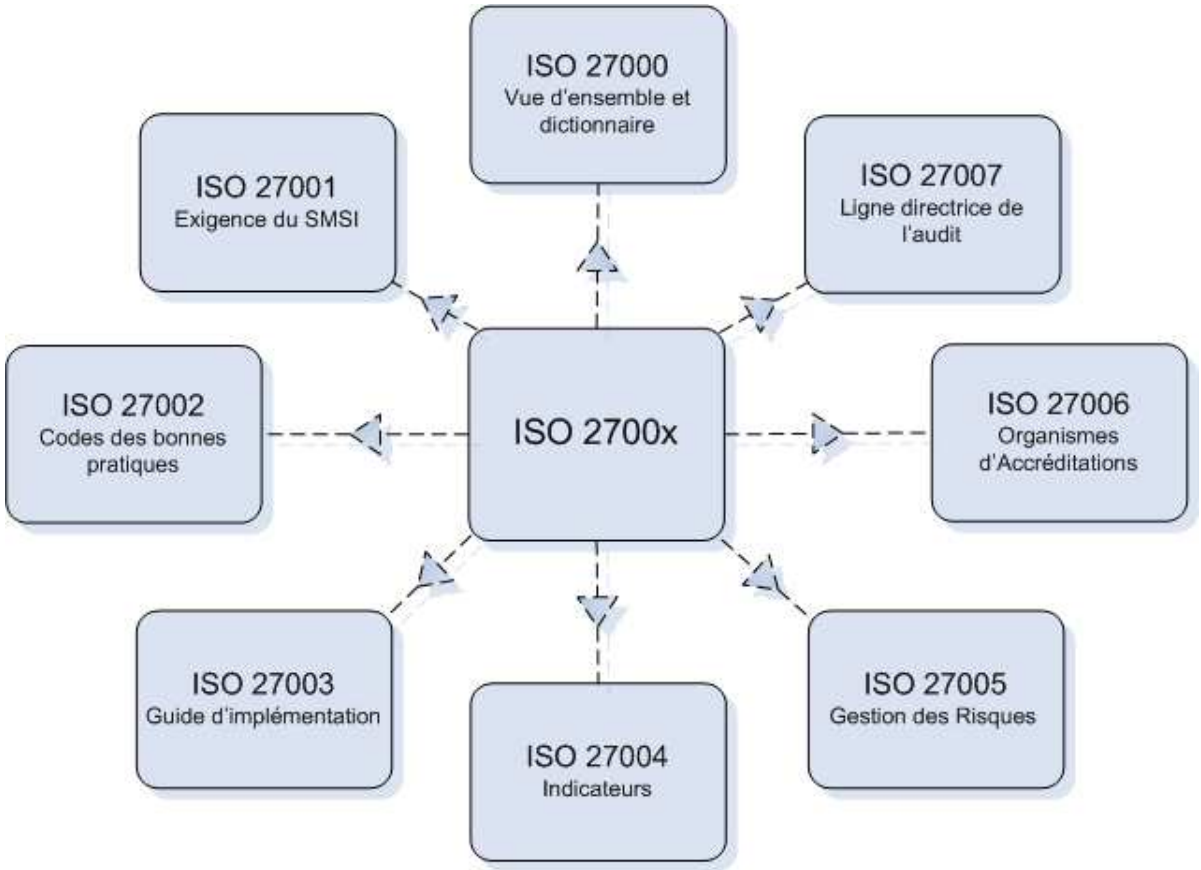
En 2000, la norme BS7799-1, devient la norme de référence internationale pour les organismes souhaitant renforcer leur sécurité de l'information. Après avoir suivi un processus de concertation au niveau international et quelques ajouts, l'ISO lui attribue un nouveau nom, ISO/IEC 17799: 2000.

En 2002, le BSI fait évoluer la norme BS7799-2 en s'inspirant des normes ISO 9001:2000 et ISO 14001: 1996. La norme adopte définitivement une approche de management de la sécurité de l'information.

En 2005, l'ISO/CEI adopte la norme BS7799-2 sous la référence ISO/CEI 27001: 2005 en y apportant quelques modifications pour se rapprocher le plus possible du principe de «système de management » développé par les normes ISO 9001 et ISO14001. L'ISO/IEC 27001: 2005 spécifie les exigences pour la mise en place d'un SMSI (système de management de l'information).

En 2007, dans un souci de clarification, l'ISO renomme la norme ISO/IEC 17799 :2005 en changeant sa numérotation pour ISO/IEC 27002. La norme se greffe à la famille des normes ISO/IEC 2700x toujours en développement.

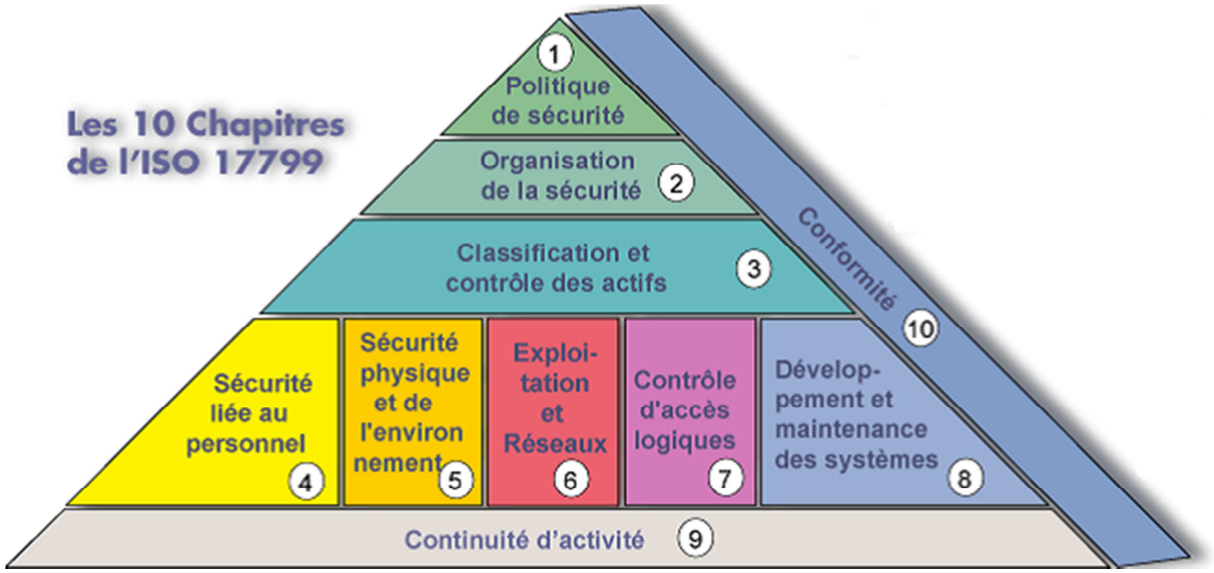
Aujourd'hui les organismes disposent de deux normes qui se sont imposées comme référence des SMSI, l'ISO/CEI 27001 :2005 qui décrit les exigences pour la mise en place d'un SMSI et l'ISO/CEI 27002 qui regroupe un ensemble de bonnes pratiques «best practices» pour la gestion de la sécurité de l'information.
Autour de ces deux normes viennent s'articuler d'autres normes de la même famille, ISO/CEI 2700x, encore en développement pour certaines .



ISO 2700x : une famille de normes pour la gouvernance sécurité

Les normes sont utilisées dans tous les actes de la vie économique. Elles représentent un langage commun et un lien nécessaire entre les divers acteurs concernés. Aujourd'hui, la normalisation s'intéresse fortement au domaine de la sécurité de l'information en proposant un modèle de gouvernance par l'intermédiaire de la norme ISO/IEC 27001 et de la certification associée.

Norme 27002



Cette nome ou code de bonne pratique est subdivisé en différentes 10 chapitres

Chapitre 1 : Politique de sécurité

La politique de sécurité donne des définitions claires de la sécurité de l'information (SI), une explication des principes de sécurité, évoque l'implication de la direction de l'organisme et les modalités de déclaration des incidents de sécurité.

On retiendra que les facteurs clé de succès de la mise en œuvre d'une politique de sécurité de l'information sont :

- la mise en œuvre de la gestion de la SI compatible avec la culture de l'organisation
- un soutien et un engagement réel et visible de la direction de l'organisme
- une bonne compréhension des exigences de sécurité
- une bonne communication interne (auprès des employés et des responsables) (présentation – formations – campagnes de sensibilisation)
- une bonne communication externe de la politique de SI (auprès des fournisseurs par exemple)
- un système de mesures pour évaluer l'efficacité de la gestion de la sécurité

Chapitre 2 : Organisation de la sécurité

Des groupes de travail devront être mis en œuvre, avec l'appui de la direction, pour approuver la politique de sécurité de l'information, pour assigner des rôles de sécurité et pour coordonner la sécurité dans l'organisme.

Chapitre 3 : Classification et contrôle des actifs

La norme préconise qu'un propriétaire soit identifié pour chaque actif principal (exemple: Données client, données achat, …) de façon à s'assurer qu'un niveau de protection approprié de cet actif soit mis en œuvre. Ce propriétaire d'information sera responsable de la mise en œuvre des contrôles appropriés et même si la réalisation des contrôles peut être déléguée, la responsabilité finale vis-à-vis de cet actif devra demeurer chez le propriétaire désigné.

Le processus de réalisation de l'inventaire des actifs est un aspect important de la gestion des risques. Un organisme doit pouvoir identifier ses actifs, ainsi que leur valeur et importance relatives.

Chapitre 4 : Sécurité liée au personnel

La norme ne se réduit pas à une norme technique, elle met beaucoup l'accent sur la culture de la sécurité de l'entreprise et notamment celle liée à son personnel, notamment lors de la procédure de recrutement, des contrats d'embauche et de la formation à la sécurité (connexions et déconnexion aux applicatifs, politique de mots de passe, signalement des incidents de sécurité, processus disciplinaire).

Chapitre 5 : Sécurité physique et de l'environnement

Sécurité Physique :

La sécurité physique est un sujet de fond dans la sécurité de l'information. La norme préconise la création de différents niveaux de sécurisation de zone, la mise en place de systèmes de contrôle d'accès, la séparation des zones de livraison…

Sécurité du matériel informatique :

La norme aborde les thèmes liés à la sécurité des serveurs et de leur environnement (gestion des alimentations électriques, politique pour limiter l'utilisation de boisson et de nourriture, procédure de sortie des matériels informatiques des locaux…)

Des points plus sensibles sont abordés comme par exemple : comment effacer définitivement les données ?

Chapitre 6 : Sécurité de l'exploitation et des réseaux

Dans ce chapitre, deux grands thèmes sont décrits :

- les thèmes liés à la sécurisation de l'exploitation de l'information (évolutions des systèmes d'information, gérer les incidents de sécurité, séparation des fonctions à risques…)
- la sécurité des réseaux au sens large véhiculant l'information, notamment toute la sécurité des échanges et les moyens associés (scellement, cryptographie, signature électronique…)

Chapitre 7 : Contrôles d'accès logique

Ce chapitre décrit la politique à mettre en œuvre pour structurer la gestion des accès au système d'information pour les utilisateurs de l'organisme, mais également pour les systèmes externes qui se connectent automatiquement à des applications.

Deux thèmes sont abordés :

- la gestion des mots de passe
- la gestion des accès logiques

Chapitre 8 : Développement et maintenance des systèmes d'information

Ce chapitre traite des infrastructures informatiques, des applications de l'entreprise et également des applications développées par les utilisateurs. Mais aussi de la politique sur l'utilisation des mesures cryptographiques : cette partie décrit l'ensemble du processus organisationnel à mettre en œuvre pour assurer une bonne utilisation du cryptage, des signatures numériques, des services de non répudiation et de la gestion des clés.

Chapitre 9 : Continuité d'activité

Quelles que soient les probabilités de risques, les dirigeants doivent pouvoir engager des moyens pour garantir la continuité de l'activité et en particulier, la permanence de la relation client. Sans système d'information, l'entreprise a en effet bien du mal à réorganiser ses processus. Cette conception dépasse la reprise sur le seul sinistre du système d'information : elle vise à réunir pour chaque collaborateur un emplacement de travail, un téléphone, et un poste de travail.

Chapitre 10 : La gestion de la conformité

Comme l'ISO 177999 est une norme internationale, l'identification de la législation applicable au pays est la première tâche. Il convient ensuite de définir explicitement et documenter les exigences légales, réglementaires et contractuelles pour chaque système d'information. (Propriété intellectuelle, droits d'auteur, copyright des logiciels, protection des données personnelles…)

<u>Normes ISA 99 :</u> Cyber sécurité des systèmes de contrôle

Le monde du contrôle de procédé a intégré les technologies de l'informatique, et la cyber sécurité devient une composante essentielle de la sécurité fonctionnelle (au moment où les standards IEC 61508 et normes filles sont sortis les technologies de contrôle restaient spécifiques et le problème était marginalisé).La cyber sécurité correspond à une lutte contre un certain type d'agression externe et devient une discipline à part entière.

La nome ISA 99 a trait à la prévention des risques associés aux intrusions dans le système de contrôle –commande, liées à des actions malintentionnées au travers des équipements.

Les principes généraux de sécurité de l'informatique industrielle sont développés dans la norme SP-99

- *Les documents qui l'accompagnent (ISA-TR99.00.01, et ISA-TR99.00.02), Publiés par l'association ISA (The Instrumentation, Systems and Automation Society).*

Les standards ISA 99 :

- *Ce sont les principaux textes disponibles actuellement qui traitent de façon organisée de la sécurité de l'informatique industrielle.*
- *Ils constituent un bon point de départ pour prendre en compte de façon méthodique la problématique de la sécurisation des systèmes d'information industriels.*
- ***ISA-TR99.00.01**, « Technologies de sécurité pour le contrôle de processus » (dernière version date de 2007), qui est un « tutorial » sur les technologies du monde informatique potentiellement utilisables dans les systèmes de contrôle, permettant d'évaluer leur intérêt au regard de la capacité de résistance aux cyber-attaques.*
- ***ISA-TR99.00.02** « Intégration de la sécurité électronique dans les systèmes de contrôle de processus » (dernière version date de 2008), qui propose une approche pour auditer un système, déterminer ses failles éventuelles face aux différentes attaques dont il peut être l'objet et faciliter la vérification de la bonne application des mesures de mise en conformité face aux recommandations formulées.*
- ***ISA-TR99.00.03** « Operating an Industrial Automation and Control System Security Program» qui est prévu pour 2009. Cette partie définira comment mettre en œuvre un programme de sécurité et les moyens de contrôler son efficience (Audits et Métriques).*

Niveau d'application des normes