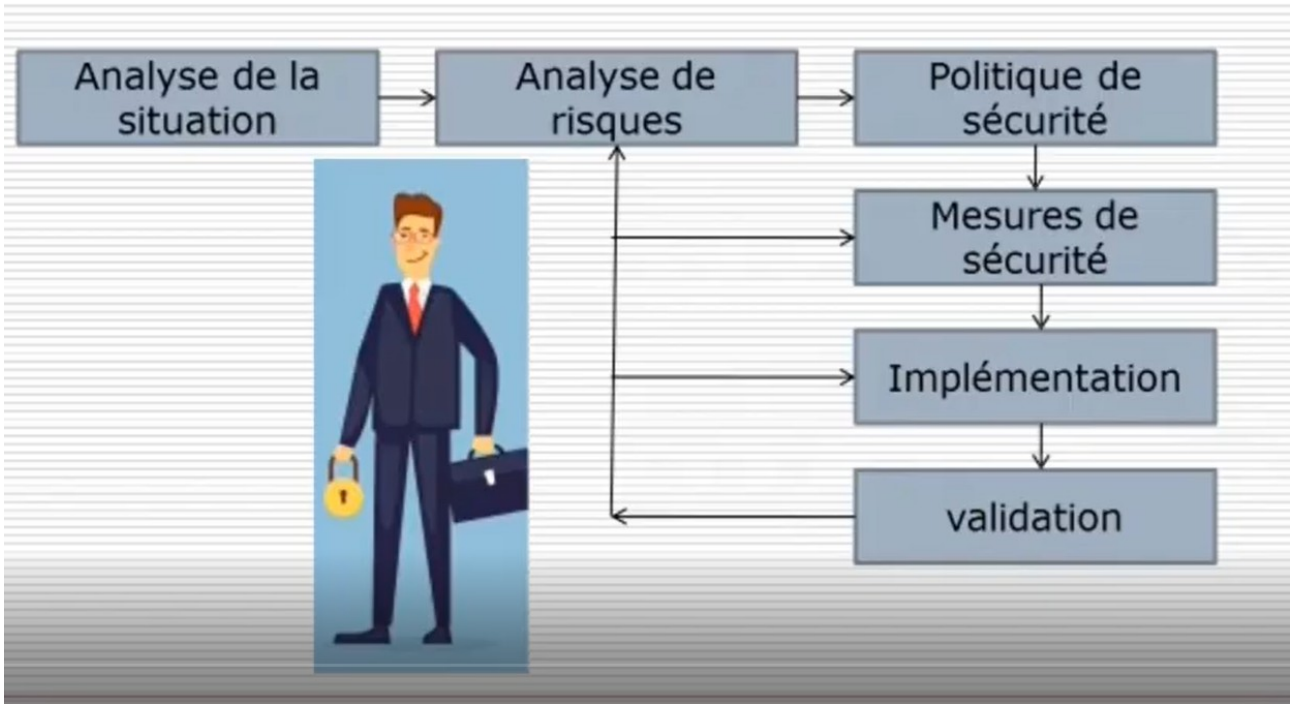
Cours2 : Cybersécurité

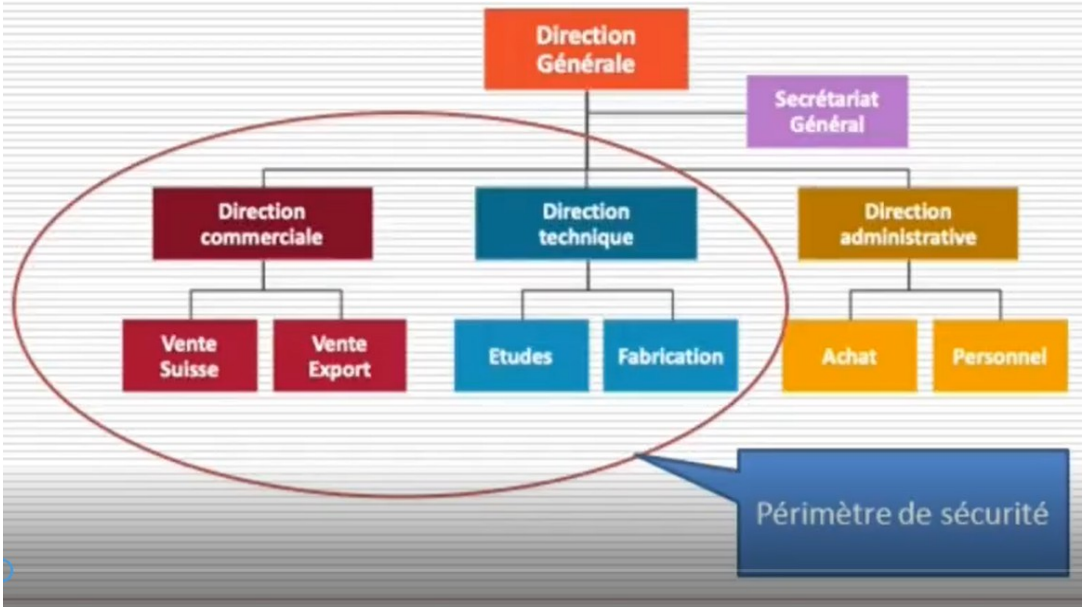
RSSI :Responsable de la **S**écurité du **S**ystème **I**nformatique

Après avoir développé dans les cours précédents, les objectifs essentiels de la sécurité informatique, on va voir quel est le métier d'un expert en sécurité informatique. On peut avoir dans une entreprise un responsable en sécurité de système d'information ou un expert en sécurité, indépendant, qui travaille à son propre compte et qui peut conclure des marchés avec des entreprises. Que ça soit un expert ou un RSSI, ils vont avoir les mêmes tâches à faire. Quelles sont les étapes globales de ces experts là sans rentrer dans les détails techniques ? Les différentes attaques techniques et les systèmes de protection seront abordés ultérieurement. Il faut garder en mémoire ce schéma là qui représente plusieurs étapes de travail. Un RSSI ou un expert en sécurité va naviguer dans ces différentes étapes.



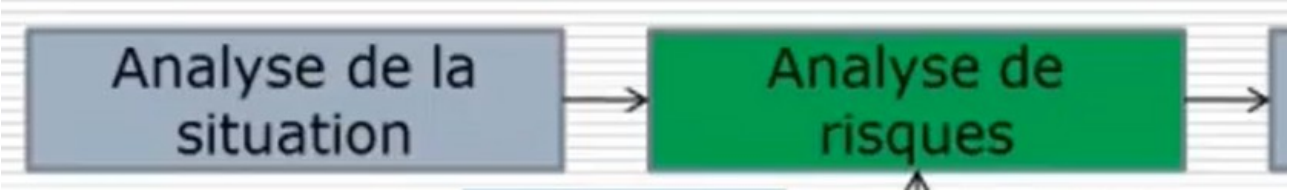
On va donc développer le contenu de chacune des étapes pour vous permettre de découvrir le métier des professionnels de la sécurité informatique. La première étape, c'est l'analyse de la situation

Analyse de la situation identifier le contexte du système à sécuriser.« *On ne sécurise pas de la même manière une maison, une banque ou une gare* »	Ça consiste à identifier le contexte. Qu'est ce que je vais protéger : une banque, une entreprise étatique ou privée, un hôpital, une université, un ministère ...Etc. Il va falloir définir le contexte. On va adopter une approche différente pour chaque contexte différent. On parle de contexte ou de périmètre.



Quelque fois nous avons à sécuriser qu'une partie de l'entreprise. Ce cercle déformé que nous avons tracé correspond au périmètre du lieu de notre sécurité. Nous avons ici à sécuriser la direction commerciale qui gère vente Suisse et vente Export, et la direction technique qui gère le bureau d'étude et de fabrication. Les autres endroits ne nous concernent pas.

La deuxième étape : l'étude de risque, est le plus important.



C'est là que le RSSI ou l'expert sécurité va faire le travail le plus délicat. Il va donc étudier les risques pour l'entreprise.

- Il est nécessaire de réaliser une analyse de risque en prenant soin **d'identifier les problèmes potentiels** avec les **solutions** avec les **coûts** associés.
- L'ensemble des solutions retenues doit être organisé sous forme d'une **politique de sécurité cohérente**, fonction du niveau de tolérance au risque.
- On obtient ainsi la liste de ce qui doit être protégé.

L'objectif de cette étape est d'identifier les problèmes potentiels avec les solutions correspondantes et les coûts associés. Pourquoi faut-il définir les risques ? Parce que dans l'étape suivante, nous allons adopter une politique de sécurité. Ce travail d'analyse de risque ne va pas se faire une fois et c'est tout. Si vous êtes spécialiste de sécurité, vous aller la faire à chaque fois et y revenir plus souvent pour revérifier ces risques-là pour des raisons suivantes:

- Croissance de l'Internet
- Croissance des attaques
- Failles des technologies
- Failles des configurations
- Failles des politiques de sécurité
- Changement de profil des pirates

Vous allez revenir revérifier pour voir s’il n’y a pas de nouveaux risques, de nouvelles failles, de nouvelles attaques de la part des pirates. Et vous allez être rémunéré par rapport à ces différentes interventions.