Université ABDELMALEK ESSAADI
école National des Sciences appliquée de Tanger

Département de mathématique et informatique

Master Cyber Sécurité et cybercriminalité (MCSC)

Expression des Besoins et Identification des Objectifs de Sécurité -EBIOS

Najah Issam

année universitaire : 2019/2021

M. Ahmed El Oualkadi

Table des matières

Introduction **2**

1 Présentation de la méthode EBIOS **3**
1.1 Definition du méthode EBIOS 3
1.1.1 Étapes de la démarche 3
1.2 Avntages du méthode EBIOS 4
1.3 Inconvénients du méthode EBIOS 4

2 l'analyse des risques -EBIOS : "Bois St-Laurent" **5**
2.1 Étude du contexte 5
2.1.1 Étude de l'organisme 6
2.1.2 Étude du Système Cible 8
2.1.3 Détermination de la cible de l'étude de sécurité 9
2.2 Expression des besoins de sécurité 9
2.2.1 Réalisation des fiches de besoins 10
2.2.2 Synthèse des besoins de sécurité 11
2.3 Étude des menaces 12
2.3.1 Étude des origines des menaces 12
2.3.2 Étude des vulnérabilités 13
2.3.3 Formalisation des menaces 13
2.4 Identification des objectifs de sécurité 13
2.4.1 Confrontation des menaces aux besoins de sécurité 14
2.4.2 Formalisation des objectifs de sécurité 14
2.4.3 Détermination des niveaux de sécurité 14
2.5 Détermination des exigences de sécurité 15
2.5.1 Détermination des exigences de sécurité fonctionnelles 15
2.5.2 Détermination des exigences de sécurité d'assurance 16

Conclusion **17**

Reference **18**

Appendix **19**

Introduction

La SSI est directement associée à une appréciation et un traitement des risques. Ces risques sont qualifiés d'opérationnels car ils agissent directement sur les activités des administrations et des entreprises. En effet, l'organisme utilisant des moyens des technologies de l'information et de communication (TIC) et en particulier de l'Internet, pour réaliser ses activités et transactions commerciales, est directement concernée par la SSI.

Ce document présente une étude de gestion des risques SSI du société "Bois St-Laurent", réalisée à l'aide de la méthode EBIOS (Expression des Besoins et Identification des Objectifs de sécurité).

La première partie du document constitue le dossier de présentation de de la méthode EBIOS. La suite décrit l'analyse et l'étude de sécurité du société "Bois St-Laurent". Toutes les étapes et activités seront présentées brièvement.

Chapitre 1

Présentation de la méthode EBIOS

1.1 Definition du méthode EBIOS

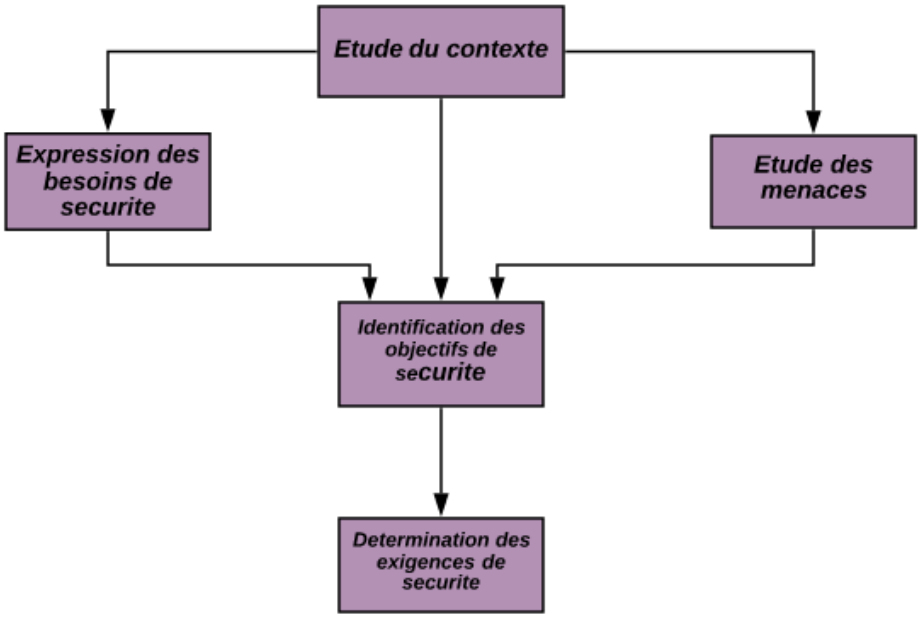
EBIOS signifie Expression des Besoins et Identification des Objectifs de Sécurité.
EBIOS est actuellement la méthode de gestion des risques de sécurité des systèmes d'information (SSI) développée et maintenue par la DCSSI (Direction centrale de la sécurité des systèmes d'information - France). Cette méthode a la particularité d'être disponible gratuitement, pour tout organisme souhaitant mener une étude des risques SSI et mettre en place une politique adéquate de sécurité de l'information. L'article présente de manière générale la méthode et ses spécificités, puis montre ses perspectives dans le domaine en plein développement que constitue la certification ISO 27001.

1.1.1 Étapes de la démarche

EBIOS est largement utilisée dans le secteur public (l'ensemble des ministères et des organismes sous tutelle), dans le secteur privé (cabinets de conseil, petites et grandes entreprises), en France et à l'étranger (Union européenne, Québec, Belgique, Tunisie, Luxembourg...), par de nombreux organismes en tant qu'utilisateurs ou bénéficiaires d'analyses de risques SSI.

l'analyse des risques avec Ebios ce fait avec les étapes de la démarche suivants :

- **Étude du contexte :** Vision globale et explicite du système étudié ,des enjeux ,des contraintes et référentiels applicables.
- **Étude des besoins :** Positionnement des éléments à protéger (patrimoine informationnel)en terme de disponibilité, intégrité ,confidentialité ... , et mise en évidence des impacts en cas de sinistre.
- **Étude des menaces :** Recensement des scénarios pouvant porter atteinte aux composants(techniques ou non)du SI.
- **Identification des objectifs de sécurité :** Mise en évidence des risques réels et expression de la volonté de les traiter en cohérence avec le contexte particulier de l'organisme.
- **Détermination des exigences de sécurité :** Spécification des mesures concrètes à mettre en œuvre pour traiter les risques sur la base d'une négociation argumentée.



1.2 Avntages du méthode EBIOS

la méthode EBIOS fourni les avantages suivants :

- Le logiciel est gratuit et disponible sur simple demande auprès de la DCSSI.
- Une méthode claire : elle définit clairement les acteurs, leurs rôles et les interactions.
- Une approche exhaustive : contrairement aux approches d'analyse des risques par scénarios, la démarche structurée de la méthode EBIOS permet d'identifier les éléments constitutifs des risques.
- Une démarche adaptative : la méthode EBIOS peut être adaptée au contexte de chacun et ajustée à ses outils et habitudes méthodologiques grâce à une certaine flexibilité.
- Un seul et même outil permet de réaliser différentes démarches sécuritaires liées à la gestion des risques SSI.

1.3 Inconvénients du méthode EBIOS

la méthode EBIOS a également des inconvénients :

- La méthode EBIOS ne fournit pas de recommandations ni de solutions immédiates aux problèmes de sécurité.
- Il n'y a pas d'audit et d'évaluation de la méthode.
- La méthode EBIOS ne fournit pas de recommandations ni de solutions immédiates aux problèmes de sécurité.
- Il n'y a pas d'audit et d'évaluation de la méthode.

Chapitre 2

l'analyse des risques -EBIOS : "Bois St-Laurent"

le groupe de travail

le groupe de travail est nécessaire pour faire une étude de risque avec EBIOS.
Ce groupe de travail devrait être hétérogène et représentatif des utilisateurs et propriétaires du système d'information (responsables, informaticiens et utilisateurs). Celui-ci va pouvoir discuter et établir un consensus sur les besoins de sécurité et de leur justification dans l'organisation.
pour notre exemple de société "Bois St-Laurent" on a deux Responsables : (Responsable de l'informatique, Représentant des superviseurs)et un directeur de l'usine.

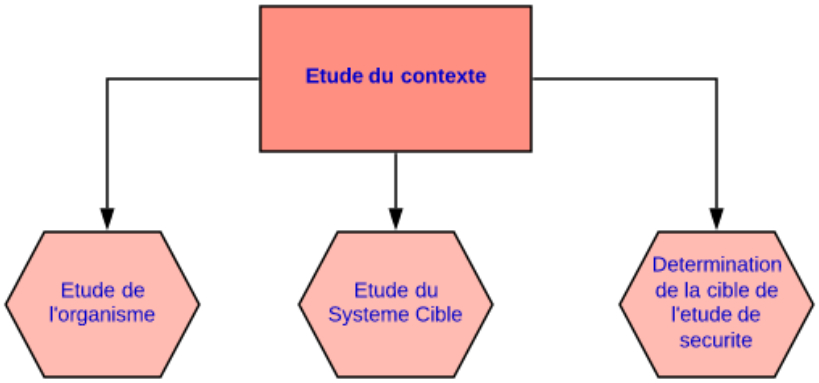
2.1 Étude du contexte

buts principales :

- étude globalement le système-cible .
- prise de connaissance du domaine à étudier .
- situer système-cible dans son environnement .
- déterminer précisément la cible-d'étude.
- préciser enjeux , contexte , mission/service , moyens.
- Réunir les informations nécessaires à la planification de l'étude

résultats :

- les champs d'investigation de l'étude est clairement délimite.
- les obligations et les contraintes sont recensées.
- les sujets a traiter sont connus.



on peut diviser cette parie on Trois activités :

- Étude de l'organisme.
- Étude du système cible.
- Détermination de la cible de l'étude.

2.1.1 Étude de l'organisme

Cette activité consiste à définir le cadre de l'étude. Des informations générales sur l'organisme concerné par le projet de sécurité doivent donc être réunies dans le but de mieux apprécier sa nature, son organisation et les contraintes qui pèsent sur celui-ci. Il est aussi nécessaire d'obtenir .

- Données en Entrée : Plan stratégique, bilan d'activité, charte sécurité.
- Données Sortie : place système dans organisation, liste contraintes.

o Présentation de l'organisme

dans cette partie on doit rappeler les éléments caractéristiques qui définissent l'identité d'un organisme. Il s'agit de la vocation, du métier, des missions, des valeurs propres et des axes stratégiques de cet organisme.

notre exemple c'est la société Bois St-Laurent :

Bois St-Laurent est une scierie (usine de production de bois d'œuvre utilisé dans la construction résidentielle) créée en 1954 dans la région de La Tuque, en Mauricie, au Québec (Canada). L'usine est un établissement d'un grand groupe industriel, Bois St- Laurent, dont le siège social est situé à Montréal. Le groupe a été acheté récemment par la société multinationale Suédoise principalement active dans le secteur forestier. Elle emploi aux environs de 800 ouvriers dont la majorité sont des ouvriers non qualifiés travaillant en continu (3 quarts de travail de 8 h).

o Contraintes de l'organisme

Il s'agit de prendre en compte l'ensemble des contraintes qui pèsent sur l'organisme et qui pourront déterminer des orientations en matière de sécurité.

par exemple Contraintes d'ordre budgétaire :

Budget total du projet de 1 500 000$
Contraintes fonctionnelles :
L'usine doit fonctionner 7 jours semaines et 24 heures par jour.

o Références réglementaires générales

La prise en compte des lois, règles ou règlements, peut modifier l'environnement, les habitudes de travail, l'accomplissement des missions ou avoir une influence sur l'organisation interne.

Par exemple le fonctionnement d'administrations de l'État est régi par des codes spécifiques (Loi sur la santé et sécurité du travail du Québec : La Loi sur la santé et la sécurité du travail Québec oblige les employeurs à prendre les mesures nécessaires pour protéger la santé et assurer la sécurité et l'intégrité physique des salariés. En vertu de cette loi, les employés peuvent refusé d'exécuter un travail dangereux.).

o Architecture du SI

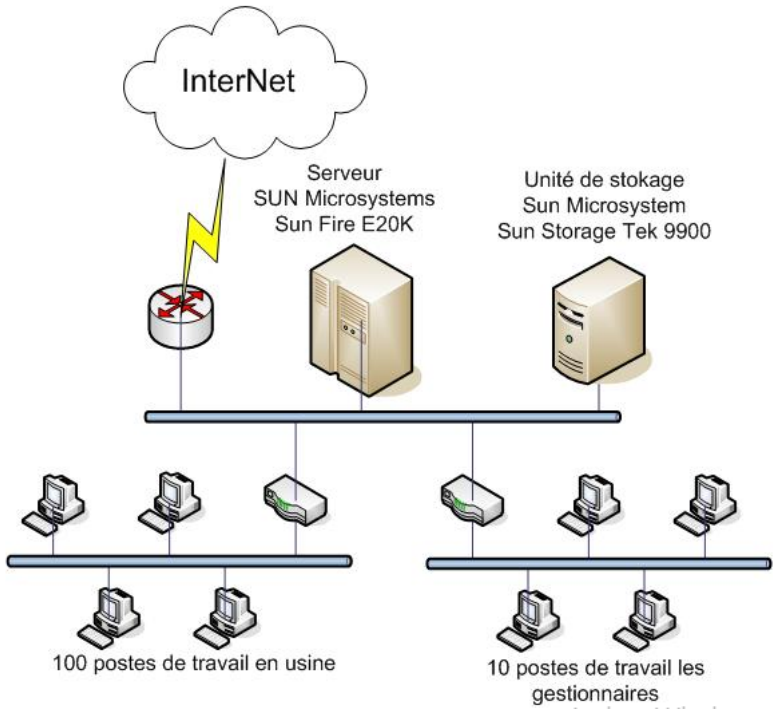
Il s'agit d'identifier les domaines fonctionnels qui contribuent à l'atteinte des objectifs stratégiques et leurs interactions. On s'efforce à ce niveau de représenter les interactions existantes et/ou futures des domaines fonctionnels avec le domaine auquel le système-cible appartient.
on peut diviser cette étape on 3 parties :

• Domaines d'activité : généralement cette partie permet la gestion l'intégration des fiches lie aux acteurs internes de l'entreprise. par exemple (Gestion du respect des consignes contenues sur la fiche. Superviseurs.).

• Acteurs externes : généralement cette partie est relié avec tous ce qui externe de l'entreprise ,(Gestionnaires forestiers : Les billes de bois sont acheminées de la forêt par camion et livrés à l'usine par des Gestionnaires de forêt privés.).

• Schéma : c'est la topologie réseau de société , et comment les matériels informatique sont placé dans l'entreprise.

Schéma



le réseau d'entreprise Bois St-Laurent se compose d'un routeur connecté a l'internet , en plus de deux switch , le premier pour les postes de travail d'usine et le deuxième pour postes de travail les gestionnaires.en plus d'un serveur et d'une unité de stockage SUN microsysteme.

2.1.2 Étude du Système Cible

Cette activité a pour but de préciser le contexte d'utilisation du système à concevoir ou existant. Pour cela, il est nécessaire de préciser le sous-ensemble du système d'information de l'organisme constituant le système-cible de l'étude et ses enjeux. Le système-cible est alors décrit et sont recensées les hypothèses, les règles de sécurité et ses contraintes.

• Données en Entrée : relations entre domaines d'activité du SI, liens inter-domaines, évolution, priorités, évaluation risques stratégiques.
• Données Sortie : Architecture conceptuelle du SI, relations fonctionnelles avec systèmecible, Définition du "système essentiel" du système-cible, Sélection enjeux .

o Présentation du système-cible

Le système-cible doit faire l'objet d'une description synthétique qui met clairement en évidence son périmètre, ses relations avec les autres domaines ou acteurs externes et ses finalités au sein du système d'information global.

Système-cible	
Présentation	Projet SIGES: système intégré de gestion d'entreprise relié au système de gestion central SAP, situé en Suède.

o Enjeux

À ce stade de la réflexion, les objectifs stratégiques sont censés être connus (cf. schéma directeur informatique, étude d'opportunité. . .), les besoins fonctionnels ciblés et définis, les contraintes informationnelles et organisationnelles du système-cible répertoriées. Il convient dès lors d'analyser les enjeux et le contexte dans lequel se situe le système-cible.

o Sélection du système-cible

Domaines d'activité du système-cible	
Intégration des fiches	*Intégration au système d'information. Techniciens en administration*

o Éléments essentiels

Les éléments essentiels sont généralement les fonctions et informations au cœur de l'activité du système-cible. Il est aussi possible de considérer d'autres éléments essentiels tels que les processus de l'organisme. Cette seconde approche sera plus appropriée dans le cadre d'élaboration d'une politique de sécurité des systèmes d'information, d'un schéma directeur de sécurité des systèmes d'information ou d'un plan de continuité. Les éléments essentiels constituent le patrimoine informationnel ou les "biens immatériels" que l'on souhaite protéger. Selon leur finalité, certaines études ne mériteront pas une analyse exhaustive de l'ensemble des éléments composant le système cible. Dans ce contexte, le périmètre de l'étude pourra être limité aux éléments vitaux du système cible.

o Mode d'exploitation de sécurité

Multiniveaux	
Niveau	3
Description	Le mode d'exploitation du système est du type multiniveaux. Les personnes ayant accès au système ne sont pas toutes habilitées au plus haut niveau de classification et elles n'ont pas toutes un besoin commun d'en connaître (ou équivalent) pour les informations traitées, stockées ou transmises par le système.

2.1.3 Détermination de la cible de l'étude de sécurité

Cette activité a pour but la détermination précise des entités sur lesquelles s'appuient réalisation mesures sécurité. L'activité consiste à recenser et décrire les différentes entités, qu'elles soient de type matériel, logiciel, réseau, personnel, site ou organisation.

o Entités

Le système-cible se compose d'un assemblage d'entités techniques et non techniques qu'il convient d'identifier et de décrire. Ces entités possèdent des vulnérabilités que des méthodes d'attaque pourront exploiter, portant ainsi atteinte aux éléments essentiels, immatériels, du système-cible (fonctions et informations). Ce sont donc ces entités qu'il faudra sécuriser. Celles-ci peuvent être de différents types.

par exemple de réseau local d'entreprise :

LAN	
Type	RES_INT : Interface de communication
Description	Réseau local 100-baseT commuté à haut débit

o Relations entités / éléments

Cette tâche permet de mettre en évidence :

- les liens entre les fonctions essentielles et les entités qui contribuent à la réalisation de ces fonctions pour le système-cible,
- les liens entre les informations essentielles et les entités qui concourent au traitement de ces informations pour le système-cible.

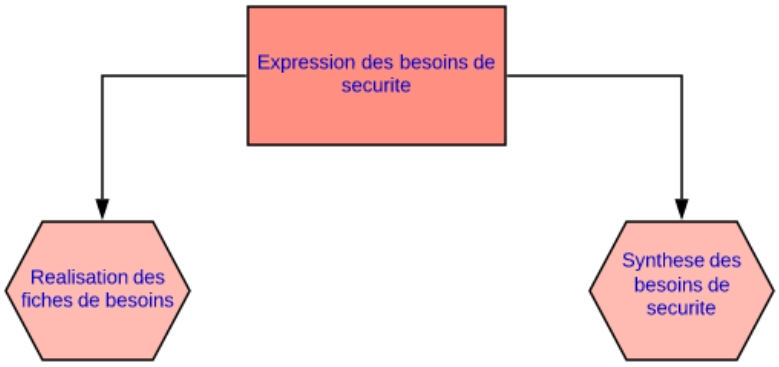
par exemple pour les fichier et les tableaux sont géré par logiciel SAP , DRHPERSO a un relation avec le serveur ...

2.2 Expression des besoins de sécurité

objectifs principales :

- Sélectionner les fonctions essentielles et les informations sensibles.
- Faire exprimer les utilisateurs sur les besoins en D, I, C, NR.

Résultat : Liste validée des besoins de sécurité



Actions :

- Sélection des fonctions et des informations essentielles .
- Expression des besoins sécurité des fonctions et informations sensibles .
- Synthèse du besoin de sécurité .

2.2.1 Réalisation des fiches de besoins

dans Cette partie on va créer les tableaux nécessaires à l'expression des besoins de sécurité par les différents utilisateurs. Il permet a chaque utilisateur d'exprimer les besoins de sécurité des éléments qu'ils manipulent habituellement dans le cadre de leur activité, d'une manière objective et cohérente.
Cette activité contribuant à l'estimation des risques et à la définition des critères de risques dans le processus de gestion des risques.

o Choisir les critères de sécurité à prendre en compte

Les besoins de sécurité associés à des fonctions et informations s'expriment selon des critères de sécurité. Trois critères de sécurité sont incontournables :disponibilité (D),intégrité (I),confidentialité (C) .
dans notre cas(société "Bois St-Laurent") nous utiliserons juste le critère de disponibilité (D) pour des fins de simplification.

o Déterminer l'échelle de besoins

Les besoins de sécurité devront s'exprimer pour chaque critère de sécurité sélectionné.donc dans cette partie on va formulée une définition pour chaque niveau de besoins de chaque critère de sécurité.
L'exemple ci-dessous présente l'échelle pour les critères de sécurité disponibilité, d'intégrité et confidentialité.
Cette échelle doit être adaptée au contexte de l'étude avec la participation des personnes qui vont déterminer les besoins.

	Confidentialité	Disponibilité	Intégrité
0	Public	Aucun besoin de disponibilité	Aucun besoin d'intégrité
1	Restreint	Long terme (à préciser)	

o sinistres

dans notre exemple de société "Bois St-Laurent" nous avons sélectionne le Sinistre générique pour Critère de sécurité : Disponibilité

o Déterminer les impacts pertinents

Il est ensuite souhaitable de déterminer une liste d'impacts pertinents pour l'organisme. Ces impacts reflètent les axes stratégiques de l'organisme. Il peut s'agir par exemple de perte d'image de marque, d'infraction aux lois, de pertes financières, de révocation de personnels... Ils permettront d'envisager différents domaines pouvant être impactés et d'apporter des éléments de justification des besoins de sécurité.
dans notre cas société "Bois St-Laurent" nous avons déterminer plusieurs type d'impacts pertinents avec un petite Description , parmi c'est impacts : interruption de service , perturbation du fonctionnement interne et perturbation de fonctionnement de tiers.

2.2.2 Synthèse des besoins de sécurité

le but principale de cette partie :
• Affecter, pour chaque information et/ou sous-fonction, la valeur finale de sensibilité qui résulte de la synthèse des valeurs attribuées par les utilisateurs.
• L'auditeur reporte les valeurs de sensibilité déterminées par les utilisateurs sur la fiche "synthèse des besoins de sécurité" et détermine la valeur considérée comme la synthèse.

o Attribution des besoins de sécurité

Nous renseignons chacune des fiches en attribuant un besoin de sécurité par critère de sécurité et par impact, puis nous synthétisons ces valeurs afin d'avoir une seule valeur par critère de sécurité (Disponibilité, Intégrité, Confidentialité...).

o Synthèse des fiches de besoins de sécurité

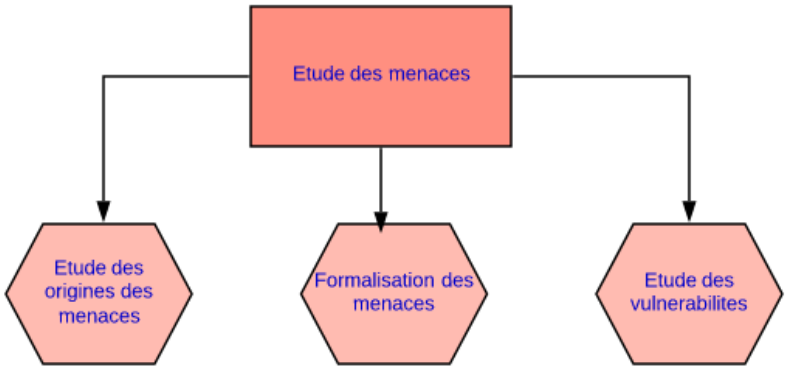
Nous rassemblons les résultats de l'expression des besoins de sécurité dans des tableaux de synthèse, soit en reprenant chaque personne interrogée, soit en sélectionnant des personnes représentatives, soit encore en effectuant un calcul (maximum ou moyenne) par type d'utilisateur. Nous synthétisons ensuite les valeurs par critère pour chaque élément essentiel et nous faisons valider les synthèses par utilisateur.

		Directeur_informatique	Directeur_usine	Rep.Supervisuers	Besoin de sécurité	Commentaires
F.FICHES	Disponibilité				3	
F.TABLEAU	Disponibilité				2	

2.3 Étude des menaces

l'objectif principale de cette étape est Déterminer les risques qui doivent être couverts par les objectifs de sécurité de la cible de l'étude.

Résultat : Liste validée des risques retenus.



Actions :

- Étude des origines des menaces.
- Étude des vulnérabilités spécifiques.
- Formalisation des menaces

2.3.1 Étude des origines des menaces

cette activité correspond à l'identification des sources dans le processus de gestion des risques. Les menaces sont sélectionnées à partir d'une liste de menaces génériques relatives à des thèmes :

- Accidents physiques
- Événements naturels
- Pertes des services essentiels
- Perturbations dues aux rayonnements
- Compromission des informations
- Défaillance technique
- Agression physique
- Fraude
- Compromission des fonctions
- Erreur

exemple risque incendie :

M.INCENDIE	
Libellé	M.INCENDIE
Méthode d'attaque	01- INCENDIE
Description	Le risque d'incendie est considéré comme significatif à l'organisation pour des raisons historiques lié au secteur d'activité.
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

2.3.2 Étude des vulnérabilités

Une vulnérabilité est une "caractéristique" du système qui peut être exploitée par une menace.
• Les vulnérabilités sont caractérisées par leur faisabilité ou leur probabilité :
* La faisabilité caractérise les vulnérabilités associées aux menaces délibérées (intentionnelles).
* La probabilité caractérise les vulnérabilités associées aux menaces accidentelles.

o les vulnérabilités retenues

Pour chaque méthode d'attaque retenue, il convient de déterminer les vulnérabilités du système-cible qui en permettent la réalisation .

o Estimer éventuellement le niveau des vulnérabilités

Les vulnérabilités peuvent être caractérisées par leur niveau, représentant la possibilité de réalisation des méthodes d'attaque qui les exploitent.
Estimer le niveau des vulnérabilités a pour objectif de ne garder que les vulnérabilités pertinentes et les hiérarchiser. On peut se contenter de les sélectionner, mais l'estimation de cette valeur permet d'obtenir un degré de finesse supplémentaire.

2.3.3 Formalisation des menaces

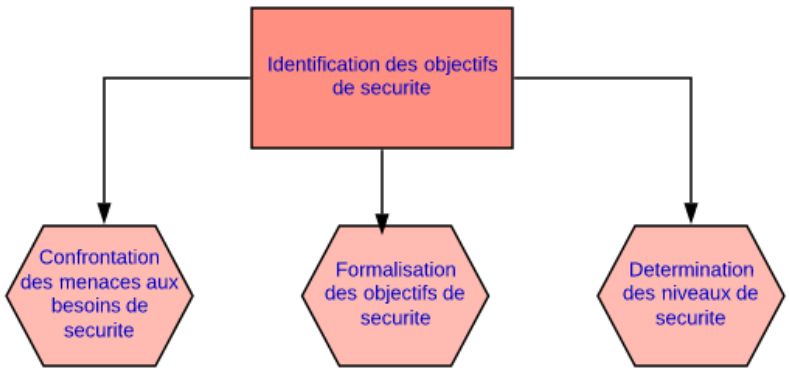
à l'issue de cette activité, il sera possible de disposer d'une vision objective des menaces pesant sur le système-cible.

o Formuler explicitement les menaces

La formulation des menaces peut être plus ou moins riche. Il s'agit avant tout d'exprimer explicitement un scénario d'attaque, le niveau de détail pouvant varier selon la finalité de l'étude.
Les menaces peuvent être caractérisées par une valeur d'opportunité déterminée selon le niveau des vulnérabilités exploitées.

2.4 Identification des objectifs de sécurité

l'objectif principale de cette étape est exprimer ce que doit réaliser la cible de l'étude pour que le système-cible fonctionne de manière sécurisé.
Resultats : Rédaction de la FEROS/Liste des objectifs de sécurité.



2.4.1 Confrontation des menaces aux besoins de sécurité

ette confrontation permet de retenir et hiérarchiser les risques qui sont véritablement susceptibles de porter atteinte aux éléments essentiels .

o calcul des besoins de sécurité concernée

Cette association est réalisée en confrontant les menaces aux besoins. D'un côté, les besoins de sécurité des éléments essentiels ont été exprimés selon différents critères de sécurité (disponibilité, intégrité, confidentialité. . .). D'un autre côté, les menaces ont été caractérisées par les critères de sécurité qu'elles peuvent affecter (d'après la caractérisation des méthodes d'attaque et selon les mêmes critères de sécurité). Il est donc possible de confronter chaque élément essentiel avec chaque menace selon les critères de sécurité afin de déterminer les conséquences possibles de la réalisation des menaces.

o Formuler explicitement les risques

En utilisant le tableau de synthèse des risques, la formulation des menaces et éventuellement l'échelle de besoins, il convient de rédiger le libellé des risques le plus explicitement possible. La finesse de la formulation dépend de la granularité souhaitée.

2.4.2 Formalisation des objectifs de sécurité

Cette activité a pour but de déterminer les objectifs de sécurité permettant de couvrir les risques, conformément à la détermination des niveaux de sécurité. La complétude de la couverture de l'ensemble des risques par les objectifs de sécurité, en prenant en compte les hypothèses, règles de sécurité et contraintes, devra être démontrée. Cette activité contribue au traitement des risques dans le processus de gestion des risques.

o Formalisation des objectifs de sécurité

O.INC- COHERENCE	
Contenu	Le site de l'usine doit disposer de mesures incendie cohérentes avec le système informatique
O.INC- ORIGINE	
Contenu	Des mesures doivent être prises pour éviter la naissance d'un incendie

2.4.3 Détermination des niveaux de sécurité

cette activité sert à déterminer le niveau de résistance adéquat pour les objectifs de sécurité. Elle permet également de choisir le niveau des exigences de sécurité d'assurance.

o Déterminer le niveau de résistance

Le niveau de résistance3 attendu des mesures de sécurité qui satisferont les objectifs de sécurité est essentiellement déterminé en fonction du potentiel d'attaque des éléments menaçants à l'origine des risques pesant sur l'organisme. En effet, le niveau de protection adéquat dépend du niveau de l'attaquant.
Nous considérons trois niveaux de résistance, exprimant les efforts minimums supposés nécessaires pour mettre en défaut le comportement de sécurité attendu par attaque directe des mécanismes de sécurité sous-jacents : Niveau élémentaire , Niveau moyen et Niveau élevé .

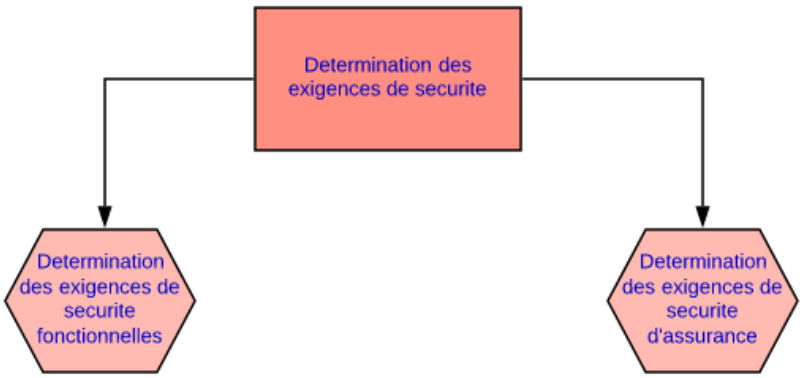
	Niveau de résistance	Justification
O.INC-COHERENCE	1	Le site doit disposer de mesures incendie cohérentes avec le système informatique, cependant niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation fortuite de la sécurité du système par des attaquants possédant un potentiel d'attaque faible
O.INC-ORIGINE	2	Des mesures doivent être prises pour éviter la naissance d'un incendie, cependant le niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation facile à mettre en oeuvre ou une violation intentionnelle de la sécurité du système par des attaquants possédant un potentiel d'attaque modéré.

o le niveau des exigences d'assurance
Il existe 7 niveaux d'assurance prédéfinis (appelés EAL – Evaluation Assurance Level) : EAL 1 ,EAL 2 ...EAL 7 .

Le niveau d'assurance EAL représente le niveau de confiance que l'on peut accorder à la mise en œuvre des objectifs de sécurité. Plus précisément, le niveau d'assurance porte sur la mise en œuvre des exigences fonctionnelles de sécurité, qui sont un raffinement des objectifs de sécurité. Plus il est élevé, plus l'organisme disposera de garanties sur celles-ci. Mais il est important de considérer le coût de la mise en œuvre des exigences d'assurance, ainsi que la faisabilité pour l'organisme ou ses fournisseurs.

2.5 Détermination des exigences de sécurité

L'équipe de mise en œuvre de la démarche doit spécifier les fonctionnalités de sécurité attendues. L'équipe chargée de la mise en œuvre de la démarche doit alors démontrer la parfaite couverture des objectifs de sécurité par les exigences fonctionnelles et les exigences d'assurance.



2.5.1 Détermination des exigences de sécurité fonctionnelles

Cette activité a pour but de déterminer les exigences de sécurité fonctionnelles permettant de couvrir les objectifs de sécurité identifiés pour le système-cible. Elle permet de décider de la manière dont chaque risque identifié devra être traité. Les risques pourront être refusés, optimisés, transférés ou pris et le risque résiduel devra être clairement identifié et accepté. Cette activité contribue au traitement des risques dans le processus de gestion des risques.

o les exigences de sécurité fonctionnelles

Les exigences de sécurité fonctionnelles représentent les moyens d'atteindre les objectifs de sécurité et donc de traiter les risques SSI afférents. Ils doivent être déterminés par ou avec la maîtrise d'œuvre (il est possible d'utiliser les exigences de sécurité fonctionnelles génériques et

le tableau de détermination des objectifs et exigences de sécurité du guide "Outillage pour le traitement des risques SSI" pour lister les exigences de sécurité fonctionnelles susceptibles de satisfaire les objectifs de sécurité couvrant les vulnérabilités identifiées).

2.5.2 Détermination des exigences de sécurité d'assurance

Cette activité a pour but l'expression complète des exigences de sécurité d'assurance de la cible de l'étude de sécurité. Elles sont sélectionnées selon le niveau d'assurance choisi lors de la détermination des niveaux de sécurité. Elles constituent le fondement de la confiance dans le fait qu'un système-cible satisfait à ses objectifs de sécurité. Cette activité contribue au traitement des risques dans le processus de gestion des risques.

o les exigences de sécurité d'assurance

Les exigences de sécurité d'assurance de l'ISO/IEC 15408 sont imposées aux actions du développeur, aux éléments de preuve produits et aux actions de l'évaluateur (exemple : contraintes sur la rigueur du processus de développement et exigences pour rechercher et analyser l'impact des vulnérabilités de sécurité potentielles).

Conclusion

L'utilisation des méthodes de gestion des risques est devenue systématique pour les entreprises soucieuses de leur sécurité. EBIOS, en tant que véritable boîte à outil de la gestion des risques, contribue à de nombreuses démarches de sécurité permettant d'élaborer le socle de la SSI (schéma directeur, politique de sécurité, tableaux de bord) et de rédiger des spécifications de sécurité (FEROS, profil de protection, cible de sécurité, politique de certification ou d'autres formes de cahiers des charges et plans d'action). La méthode EBIOS présente l'avantage de structurer une démarche complète de construction du risque, à partir de l'existant de l'organisation concernée. Associées à cette démarche, les bases de connaissance, remises à jour constamment, ainsi qu'un logiciel "open source" disponible gratuitement, fournissent un support rapide et efficace. La méthode EBIOS est souvent présentée en "concurrence", avec d'autres méthodes de gestion des risques SSI. Cependant, au-delà des comparaisons, EBIOS propose une démarche singulière de construction des risques, dégagée de toute préoccupation commerciale, et s'adaptant à tout type d'organisation, qu'elle soit privée ou publique.
Pour conclure il faut dire qu'il n'y a pas la notion de « zéro risque », les risques sont toujours existes mais grâce à l'évolution des sciences que ce soit au niveau informatique ou juridique ou n'importe quel autre domaine, on peut réduire le niveau des risques par suivi un ensemble des normes qui sont bien définies et doit respecter par chaque membre de l'organisation.

Reference :

- site wikipedia Expression des Besoins et Identification des Objectifs de Sécurité.
- ebiosv2-archimed-etudecomplete-2004-07-16.
- http ://irt.enseeiht.fr/anas/cours/ebios.pdf.

Appendix :

SSRS

Énoncé des impératifs de sécurité (System-specific Security Requirement Statement)

Libellé	Exercice 1
Organisation	Bois St-Laurent

Table des matières

1 - Introduction

2 - Définition du système ou du réseau informatique

2.1 L'organisme
2.2 Le système-cible
2.3 La cible de l'étude
2.4 Sélection des éléments essentiels
2.5 Les besoins de sécurité

3 - Définition des impératifs de sécurité

3.1 Méthodes d'attaque non retenues
3.2 Risques
3.3 Objectifs de sécurité
3.4 Niveaux de résistance

4 - Définition des environnements de sécurité

5 - Définition des mesures de sécurité

6 - Administration de la sécurité

1 - Introduction

[Un énoncé des impératifs de sécurité doit commencer par une introduction donnant une vue d'ensemble du système ou du réseau informatique et désignant les responsables de sa sécurité.]

1.1 Contexte général

[Cette section évoque brièvement le titre, le rôle, les utilisateurs, l'emplacement, les contraintes fortes et de manière générale le contexte d'utilisation. Elle doit rappeler également la raison d'être du système et l'historique qui a préludé à la décision de son développement. Dans cette section la dimension internationale du système doit être le cas échéant décrite.]

1.2 Définition des responsabilités

[Cette section identifie les différentes autorités intervenant dans le déroulement du projet :]
- autorité(s) utilisatrice(s) du système ;
- autorité chargée du projet ;
- autorité chargée de la rédaction de l'énoncé des impératifs de sécurité ;
- autorité chargée de la validation de l'énoncé des impératifs de sécurité ;
- autorité(s) chargée(s) de l'approbation de l'énoncé des impératifs de sécurité ;
- autorité chargée de l'homologation.]

1.3 Agréments et cautions

[Les besoins, connus à ce stade ou envisagés à des stades ultérieurs, pour des éléments ou parties du système devant être soumis à la procédure d'agrément ou de caution doivent être précisés.]

1.4 Évaluation

[L'utilisation dans le système de moyens ou de produits évalués (voire l'évaluation du système lui-même) doit être précisée. Dans ce cas les choix faits ou à faire (notamment celui du niveau de l'évaluation) sont indiqués.]

1.5 Homologation de sécurité

[La procédure d'homologation applicable au système (pour sa totalité ou pour des parties), est décrite et les différents intervenants identifiés. Les conditions nécessitant une ré-homologation sont également précisées (connexion à d'autres systèmes, modifications des mécanismes de sécurité...). Dans cette section, le périmètre sur lequel porte l'homologation ainsi que le niveau de classification des informations susceptibles d'être traitées par le système à l'issue de l'homologation doivent être précisés.]

1.6 Relations de la FEROS avec les autres documents relatifs au projet

[Les liens avec les autres documents relatifs au projet, notamment ceux permettant l'expression des besoins à couvrir par le système, et les documents relatifs à la sécurité (politique de sécurité, cible de sécurité, plan de sécurité...) sont précisés.]

1.7 Interconnexion de systèmes

[Les renseignements équivalents pour les autres systèmes d'information connectés sont indiqués (description succincte des systèmes, homologation, agrément, autres documents traitant de la sécurité, existence d'énoncés des impératifs de sécurité d'interconnexion pour les liaisons etc).]

2 - Définition du système ou du réseau informatique

[Le premier stade de l'établissement d'un énoncé des impératifs de sécurité doit consister à rendre parfaitement claire la définition préliminaire, peut-être purement conceptuelle, du système ou du réseau informatique, afin d'arriver à une définition concise et exempte d'ambiguïté. Cette définition doit inclure les points suivants :]
[(a) le type d'informations à stocker, traiter ou transmettre ;]
[(b) le type/ la classe d'utilisateurs ;]
[(c) les fonctions opérationnelles ;]
[(d) le besoin opérationnel concernant l'échange d'informations et/ou les interfaces avec d'autres systèmes ou réseaux informatiques.]

[Ces informations sont nécessaires non seulement comme base de l'identification des impératifs de sécurité et des premiers travaux d'élaboration de l'énoncé des impératifs de sécurité, mais aussi comme données de référence pour l'avenir.]

[La définition du système ou du réseau informatique doit comporter un élément essentiel, qui est la définition de la limite de ce système ou réseau. Cette définition peut être difficile dans le cas d'un réseau, mais elle est fondamentale dès que l'on envisage l'interconnexion de systèmes ou de réseaux informatiques. L'étendue du système ou du réseau, et donc le champ d'application de l'énoncé des impératifs de sécurité, doivent être délimités concrètement, avec une définition bien claire des passerelles vers les autres systèmes ou réseaux informatiques. Les besoins de fonctionnalités liés par exemple à une cloison pare-feu/un garde de sécurité/une passerelle devraient toujours être inclus dans le SSRS du système ou réseau informatique qu'il protège.]

[Les informations touchant à la sécurité sur le rôle opérationnel du système ou du réseau informatique sont nécessaires pour établir la base des impératifs de sécurité. Il est essentiel de créer un point de référence clairement défini indiquant le rôle du système ou du réseau informatique, le type, le volume et la classification des informations à stocker, traiter ou transmettre, et le nombre et le niveau d'habilitation des utilisateurs.]

2.1 L'organisme

Présentation de l'organisme

Organisme	
Présentation	Bois St-Laurent est une scierie (usine de production de bois d'œuvre utilisé dans la construction résidentielle) créée en 1954 dans la région de La Tuque, en Mauricie, au Québec (Canada). L'usine est un établissement d'un grand groupe industriel, Bois St-Laurent, dont le siège social est situé à Montréal. Le groupe a été acheté récemment par la société multinationale Suédoise principalement active dans le secteur forestier.

	Elle emploi aux environs de 800 ouvriers dont la majorité sont des ouvriers non qualifiés travaillant en continu (3 quarts de travail de 8 h).

Contraintes de l'organisme

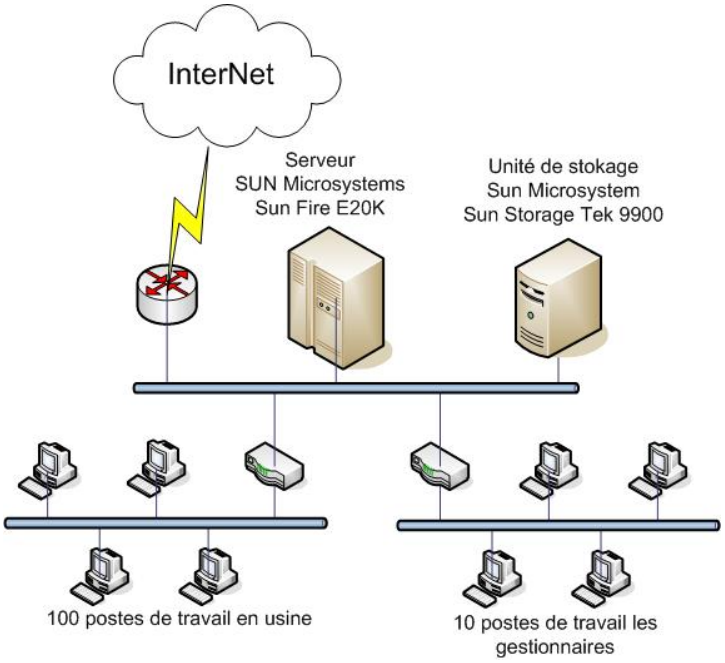
Budget total	
Thème	Contraintes d'ordre budgétaire
Description	Budget total du projet de 1 500 000$
Juin 2007	
Thème	Contraintes d'ordre calendaire
Description	Tout doit être complété pour Juin 2007.
L'usine 7/7 et 24/24	
Thème	Contraintes fonctionnelles
Description	L'usine doit fonctionner 7 jours semaines et 24 heures par jour.
Production	
Thème	Contraintes d'ordre culturel
Description	Chaque étape de la production étant organisée en atelier, dirigé par un superviseur
Syndicat	
Thème	Contraintes relatives au personnel
Description	Ateliers syndiqués.

Références réglementaires générales

LNT	
Libellé étendu	Loi sur les normes du travail du Québec
Description	La Loi sur les normes du travail du Québec établit les conditions minimales de travail en l'absence de conditions prévues par une convention collective, un contrat de travail ou un décret.
Justification	Cette loi est d'intérêt public. Les employés et la société Bois St-Laurent y sont tous soumis.
PRP	
Libellé étendu	Loi sur la protection des renseignements personnels dans le secteur privé
Description	Toute entreprise de biens et de services doit se conformer à la Loi sur la protection des renseignements personnels dans le secteur privé si elle recueille, détient, utilise ou communique des renseignements personnels.
Justification	Cette loi est d'intérêt public. Les employés et la société Bois St-Laurent y sont tous soumis.
SST	
Libellé étendu	Loi sur la santé et sécurité du travail du Québec
Description	La Loi sur la santé et la sécurité du travail Québec oblige les employeurs à prendre les mesures nécessaires pour protéger la santé et assurer la sécurité et l'intégrité physique des salariés. En vertu de cette loi, les employés peuvent refusé d'exécuter un travail dangereux.
Justification	Cette loi est d'intérêt public. Les employés et la société Bois St-Laurent y sont tous soumis.

Architecture du SI

Domaines d'activité	**Gestion des fiches des superviseurs**	
	Définition	Gestion du respect des consignes contenues sur la fiche. Superviseurs
	Liaisons	
	Gestion des fiches employée	
	Définition	Gérer la production de fiches des employés;

		Les acheminer aux employée; Récupérer les fiches à la fin des quarts de travail. Employés Techniciens en administration
	Liaisons	
	Intégration des fiches	
	Définition	Intégration au système d'information. Techniciens en administration
	Liaisons	
Acteurs externes	**Client**	
	Nom	Client
	Titre	Centre de distribution
	Description	Les produits finis sont assemblés sur des palettes et chargés sur des camions pour être expédiés à un centre de distribution.
	Liaisons	
	Fournisseurs	
	Nom	Fournisseurs
	Titre	Gestionnaires forestiers
	Description	Les billes de bois sont acheminées de la forêt par camion et livrés à l'usine par des Gestionnaires de forêt privés.
	Liaisons	
	MRNQ	
	Nom	MRNQ
	Titre	Ministère des ressources naturelles du Québec
	Description	Le Ministère est responsable de la gestion provinciale de la forêt et des quotas de bois.
	Liaisons	
Schéma		

2.2 Le système-cible

Présentation du système-cible

Système-cible	
Présentation	Projet SIGES: système intégré de gestion d'entreprise relié au système de gestion central SAP, situé en Suède.

Enjeux

H.ORGANISATION	
Description	Améliorer le climat de travail, réduire et éliminer les nombreuses grèves spontanés par l'attribution d'une plus grande autonomie pour les ouvriers par des contrat de service (Service Level Agreement ou SLA) aux groupes autonomes de quatre à six personnes en charge l'ensemble des tâches dans leur atelier.
H.TABLEAUDEBORD	
Description	Mettre en oeuvre des solutions novatrices dont un tableau de bord pour les ouvriers qui affiche les données de production relative au poste en temps réel avec l'aide de capteurs.
H.WAN	
Description	Relier l'usine au système de gestion central SAP de SWP, situé en Suède.

Sélection du système-cible

Domaines d'activité du système-cible	
Intégration des fiches	*Intégration au système d'information.* *Techniciens en administration*

Éléments essentiels

Fonction : F.FICHES	
Description	La production des fiches d'attribution ou l'attribution des tâches aux ouvriers est une fonction critique dont la perte ou la dégradation rendent la réalisation de la mission de l'usine impossible.
Fonction : F.TABLEAU	
Description	La fonction tableau de bord, tant pour les ouvriers que les gestionnaires, sont des informations stratégiques nécessaires pour atteindre les objectifs correspondants aux orientations stratégiques de SWP. La production des tableaux de bords en temps réel est une fonction essentielle critique.
Information : I.DRHPERSO	
Description	Les dossiers des employés, sont intégrés au SIG comprend des informations personnelles nominatives.
Information : I.PROD	
Description	Les données de production en temps réel sont nécessaire à la production des fiches et sont des informations stratégiques nécessaires pour atteindre les objectifs correspondants aux orientations stratégiques de SWP.

Contraintes particulières

Références réglementaires particulières

Hypothèses

Mode d'exploitation de sécurité

Multiniveaux	
Niveau	3
Description	Le mode d'exploitation du système est du type multiniveaux.

	Les personnes ayant accès au système ne sont pas toutes habilitées au plus haut niveau de classification et elles n'ont pas toutes un besoin commun d'en connaître (ou équivalent) pour les informations traitées, stockées ou transmises par le système.

Règles de sécurité

2.3 La cible de l'étude

Entités

LAN	
Type	RES_INT : Interface de communication
Description	Réseau local 100-baseT commuté à haut débit

Logiciel SAP	
Type	LOG : Logiciel
Description	le système intégré de gestion d'entreprise SAP relié par réseau privé virtuel (RPV) avec la Suède

Serveur	
Type	MAT_ACT.2 : Matériel fixe
Description	Serveur SUN Microsystems Sun Fire E20K

Relations entités / éléments

	Logiciel SAP	Serveur	LAN
F.FICHES	X		
F.TABLEAU	X		
I.DRHPERSO		X	
I.PROD			X

2.4 Sélection des éléments essentiels

Éléments essentiels	
F.FICHES	La production des fiches d'attribution ou l'attribution des tâches aux ouvriers est une fonction critique dont la perte ou la dégradation rendent la réalisation de la mission de l'usine impossible.
F.TABLEAU	La fonction tableau de bord, tant pour les ouvriers que les gestionnaires, sont des informations stratégiques nécessaires pour atteindre les objectifs correspondants aux orientations stratégiques de SWP. La production des tableaux de bords en temps réel est une fonction essentielle critique.
I.DRHPERSO	Les dossiers des employés, sont intégrés au SIG comprend des informations personnelles nominatives.
I.PROD	Les données de production en temps réel sont nécessaire à la production des fiches et sont des informations stratégiques nécessaires pour atteindre les objectifs correspondants aux orientations stratégiques de SWP.

2.5 Les besoins de sécurité

Critères de sécurité

Disponibilité	
Description	Propriété d'accessibilité au moment voulu des éléments essentiels par les utilisateurs

	autorisés. Pour une fonction : garantie de la continuité des services de traitement ; absence de problèmes liés à des temps de réponse au sens large. Pour une information : garantie de la disponibilité prévue pour l'accès aux données (délais et horaires) ; il n'y a pas de perte totale de l'information ; tant qu'il existe une version archivée de l'information, l'information est considérée comme disponible ; pour étudier la disponibilité d'une information, on suppose l'existence d'une version archivée, et on évalue la disponibilité qui correspond à la fonction d'archivage de cette information.

Échelle de besoins

	Confidentialité	Disponibilité	Intégrité
0	Public	Aucun besoin de disponibilité	Aucun besoin d'intégrité
1	Restreint	Long terme (à préciser)	
2	Confidentiel (partenaires)	Moyen terme (à préciser)	Besoin moyen d'intégrité
3	Confidentiel (interne)	Court terme (à préciser)	
4	Secret	Très court terme (à préciser)	Parfaitement intègre

Sinistres

Sinistre générique	
Critère de sécurité	Disponibilité

Impacts

interruption de service	
Description	L'incapacité pour le système de fournir le service pourra emmené des interruptions de la ligne de production
perturbation du fonctionnement interne	
Description	Le fonctionnement interne de l'organisation est perturbé avec un impact direct sur les résultats
perturbation de fonctionnement de tiers	
Description	La relation et le fonctionnement de SWP subit un impact.

Synthèse des besoins

		Directeur_informatique	Directeur_usine	Rep.Supervisuers	Besoin de sécurité	Commentaires
F.FICHES	Disponibilité				3	
F.TABLEAU	Disponibilité				2	
I.DRHPERSO	Disponibilité				3	
I.PROD	Disponibilité				4	

3 - Définition des impératifs de sécurité

[L'objectif principal de l'énoncé des impératifs de sécurité étant de servir de base à l'homologation, l'autorité d'homologation de sécurité doit être consultée pour ce qui est des impératifs de sécurité du système ou du réseau informatique dans son ensemble, en raison de sa connaissance des menaces pesant sur le système ou sur le réseau, et

compte tenu du fait que certains impératifs de sécurité constituent des normes minimales dans la doctrine de sécurité de l'OTAN.]

[L'énoncé des impératifs de sécurité peut répondre à diverses interprétations de ce que l'on entend par "sécurité d'un système ou d'un réseau informatique" ; ce n'est pas l'objet du présent document d'orientation de conseiller les services responsables du projet, les autorités d'exploitation de système informatique et les autorités d'homologation de sécurité sur la nature des impératifs de sécurité.]

[Les exigences de sécurité listées ci-dessous doivent être réparties dans cette partie du SSRS et dans la suivante.]

3.1 Méthodes d'attaque non retenues

3.2 Risques

M.ALTERATION	
Libellé	M.ALTERATION
Méthode d'attaque	36 - ALTÉRATION DES DONNÉES
Description	L'altération a été une situation problématique dans le passé, qui pourrais créer un conflit qui affectera la survie de l'usine.
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

M.DESTRUCTION	
Libellé	M.DESTRUCTION
Méthode d'attaque	05 - DESTRUCTION DE MATÉRIELS OU DE SUPPORTS
Description	La destruction de matériels ou de supports aura un impact négatif sur les dirigeants et l'usine vis-à- vis du groupe.
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

M.DIVULGATION	
Libellé	M.DIVULGATION
Méthode d'attaque	23 - DIVULGATION
Description	La divulgation de données a été une situation problématique dans le passé, surtout lors de tensions syndicales. Si cela se produisais de nouveau, cela pourrais créer un conflit qui affectera la survie de l'usine.
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

M.INCENDIE	
Libellé	M.INCENDIE
Méthode d'attaque	01- INCENDIE
Description	Le risque d'incendie est considéré comme significatif à l'organisation pour des raisons historiques lié au secteur d'activité.
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

M.PERTE- ALIMENTATIONer	
Libellé	M.PERTE- ALIMENTATIONer
Méthode d'attaque	12 - PERTE D'ALIMENTATION ÉNERGÉTIQUE
Description	Compte tenu de la situation de l'usine en région, il y a eu plusieurs pannes dans le passé. Les dirigeants de l'usine y sont particulièrement sensible suite à un incident qui a eu lieu en 1998.
Opportunité	Moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique

M.PERTE-TELECOM	
Libellé	M.PERTE-TELECOM
Méthode d'attaque	13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION

Description	La perte de télécommunications pourra interrompre le lien avec la Suède ce qui pourra influencer sur le rôle que souhaite se donner les dirigeants au sein du groupe.
Opportunité	Faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré

3.3 Objectifs de sécurité

Ce chapitre récapitule la totalité des objectifs de sécurité permettant de traiter les risques identifiés lors de l'analyse des risques. Ils résultent de la décision de l'utilisateur qui considère que leur réalisation est nécessaire pour couvrir les besoins de sécurité qu'il a exprimés et qui nécessitent leur validation par son autorité.

L'expression des objectifs de sécurité s'effectue à partir des éléments exprimés dans les chapitres précédents, ce qui signifie qu'ils proviennent du résultat de l'analyse de risque, du choix du mode d'exploitation de sécurité, de la prise en compte de l'ensemble des contraintes et de la mise en application du contexte réglementaire imposé.

Les objectifs de sécurité se répartissent dans trois domaines d'application :
- les objectifs de sécurité organisationnels (concernent l'organisation de la sécurité, la PSSI, la gestion des risques SSI, l'intégration de la SSI dans le cycle de vie des systèmes et l'assurance et la certification) ;
- les objectifs de sécurité de mise en oeuvre (concernent les aspects humains, la planification de la continuité des activités, la gestion des incidents, la sensibilisation et la formation, l'exploitation et les aspects physiques et environnement) ;
- les objectifs de sécurité techniques (concernent l'identification / authentification, le contrôle d'accès logique aux biens, la journalisation, les infrastructures de gestion de clés cryptographiques et les signaux compromettants).
Ces objectifs peuvent bien entendu s'affiner entre la phase de faisabilité et la phase de définition du système d'information concerné.

[Les objectifs de sécurité suivants doivent être réorganisés selon les trois domaines d'application ci-dessus :]

O.INC- COHERENCE	
Contenu	Le site de l'usine doit disposer de mesures incendie cohérentes avec le système informatique
O.INC- ORIGINE	
Contenu	Des mesures doivent être prises pour éviter la naissance d'un incendie
O.INC-CSQ	
Contenu	Des mesures doivent être prises pour réduire l'effet d'un incendie sur les éléments essentiels et en termes de pertes financières
O.TELECOM	
Contenu	Les dysfonctionnements des réseaux externes ne doivent pas gêner l'utilisation de Internet par les utilisateurs de l'usine
O.TELECOM- CSQ	
Contenu	Des mesures doivent être prises pour réduire l'effet des dysfonctionnements des réseaux externes sur les éléments essentiels et en termes de perturbation du fonctionnement interne
O.TELECOM- ORIGINE	
Contenu	Des mesures doivent être prises pour éviter les dysfonctionnements des réseaux externes

3.4 Niveaux de résistance

	Niveau de résistance	Justification
O.INC-COHERENCE	1	Le site doit disposer de mesures incendie cohérentes avec le système informatique, cependant niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation fortuite de la sécurité du système par des attaquants possédant un potentiel d'attaque faible
O.INC-ORIGINE	2	Des mesures doivent être prises pour éviter la naissance d'un incendie, cependant le niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation facile à mettre en oeuvre ou une

		violation intentionnelle de la sécurité du système par des attaquants possédant un potentiel d'attaque modéré.
O.INC-CSQ	2	Des mesures doivent être prises pour réduire l'effet d'un incendie sur les éléments essentiels et en termes de pertes financières , cependant le niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation facile à mettre en oeuvre ou une violation intentionnelle de la sécurité du système par des attaquants possédant un potentiel d'attaque modéré.
O.TELECOM	3	Les dysfonctionnements des réseaux externes ne doivent pas gêner l'utilisation de Internet par les utilisateurs, cependant le niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation délibérément planifiée ou organisée de la sécurité du système par des attaquants possédant un potentiel d'attaque élevé.
O.TELECOM-CSQ	2	Des mesures doivent être prises pour réduire l'effet des dysfonctionnements des réseaux externes sur les éléments essentiels et en termes de perturbation du fonctionnement interne, cependant le niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation facile à mettre en oeuvre ou une violation intentionnelle de la sécurité du système par des attaquants possédant un potentiel d'attaque modéré.
O.TELECOM-ORIGINE	2	Des mesures doivent être prises pour éviter les dysfonctionnements des réseaux externes, cependant le niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation facile à mettre en oeuvre ou une violation intentionnelle de la sécurité du système par des attaquants possédant un potentiel d'attaque modéré.

4 - Définition des environnements de sécurité

[Les termes utilisés pour distinguer les différentes zones de responsabilité et matière de sécurité d'un système ou d'un réseau informatique sont les suivants :]
[(a) environnement de sécurité global (GSE): environnement physique général de sécurité dans lequel se trouve le système ou le réseau informatique; Dans certaines configurations en réseau, il peut être constitué de plusieurs environnements globaux disjoints. Il peut y avoir matière à interprétation, et la question doit être traitée cas par cas ;]
[(b) environnement de sécurité local (LSE): environnement de sécurité (sécurité physique, sécurité du personnel, sécurité des documents, sécurité des procédures) relevant de l'autorité d'exploitation du système informatique (gestionnaire de système) ;]
[(c) environnement de sécurité électronique (ESE): environnement de sécurité du système ou du réseau informatique lui-même (par exemple, interface homme-machine, interfaces internes et externes, ponts-levis, gardes de sécurité et passerelles).]

[Toutes les mesures de sécurité identifiées doivent être applicables à ces environnements. Dans certains cas, et pour certains impératifs, il peut être approprié d'adopter un découpage plus fin, par exemple en divisant le LSE en zones de classe I, zone de classe II et zones administratives ou en divisant l'ESE en domaines de différent niveau d'assurance.]

[Les objectifs de sécurité suivantes doivent être réparties selon les environnements ci-dessus.]

O.INC- COHERENCE	
Contenu	Le site de l'usine doit disposer de mesures incendie cohérentes avec le système informatique
O.INC- ORIGINE	
Contenu	Des mesures doivent être prises pour éviter la naissance d'un incendie
O.INC-CSQ	
Contenu	Des mesures doivent être prises pour réduire l'effet d'un incendie sur les éléments essentiels et en termes de pertes financières
O.TELECOM	
Contenu	Les dysfonctionnements des réseaux externes ne doivent pas gêner l'utilisation de Internet par les utilisateurs de l'usine
O.TELECOM- CSQ	
Contenu	Des mesures doivent être prises pour réduire l'effet des dysfonctionnements des

	réseaux externes sur les éléments essentiels et en termes de perturbation du fonctionnement interne
O.TELECOM- ORIGINE	
Contenu	Des mesures doivent être prises pour éviter les dysfonctionnements des réseaux externes

5 - Définition des mesures de sécurité

[Un principe clé de la sécurité est que les différents aspects de sécurité (sécurité physique, sécurité du personnel, sécurité des documents, sécurité des procédures, sécurité informatique et sécurité des télécommunications), de la confidentialité, de l'intégrité et de la disponibilité doivent être mis en ?uvre comme une entité unique, afin d'assurer un niveau de protection cohérent des informations et des systèmes et moyens de communication.]

[L'énoncé des impératifs de sécurité présente une approche intégrée de la sécurité, indiquant les impératifs de sécurité de haut niveau du système ou du réseau informatique avant d'exposer les mesures particulières à prendre pour satisfaire à ces impératifs.]

[La présentation des mesures de sécurité détaillées doit être structurée.]

EF.LOCAUX	
Description	Les personnes extérieures entrant dans la partie « métier » du cabinet d'études doivent être accompagnées. Les personnels de maintenance, de nettoyage ou toute autre personne extérieure au cabinet d'études ne doivent pas pénétrer dans les locaux en l'absence des membres du cabinet d'études. Les locaux doivent être protégés par des serrures de sécurité dont les clés ne sont détenues que par le Directeur et son adjoint.
EF.CHIFFREMENT	
Description	Les échanges de courriers électroniques doivent être protégés en confidentialité par une solution de chiffrement disponible sur le marché. Les outils utilisant les clés de chiffrement doivent bénéficier d'une politique de gestion de ces clés.
EF.INC-DETECT	
Description	Les locaux doivent être équipés d'un système de détection d'incendie muni d'une remontée d'alarme vers une supervision externalisée. Ces mesures doivent être étudiées et mises en place par des experts du domaine. Elles doivent être testées au moins une fois par an.
EF.INC-ORIGINE **EF.INC-ORIGINE**	
Description	Un système de gicleurs centralisé doit être mis en place pour éviter la naissance d'un incendie. Ces mesures doivent être étudiées et mises en place par des experts du domaine. Elles doivent être testées au moins une fois par an.
EF.MAINTENANCE	
Description	Un contrat de maintenance doit garantir la disponibilité des moyens de communication internes et externes dans un délai conforme aux enjeux (1 heure d'indisponibilité)
EF.TELECOM	
Description	Les dysfonctionnements des réseaux externes ne doivent pas gêner l'utilisation de Internet par les utilisateurs, cependant le niveau de la résistance tel que l'analyse montre que la fonction concernée fournit une protection adéquate vis-à-vis d'une violation délibérément planifiée ou organisée de la sécurité du système par des attaquants possédant un potentiel d'attaque élevé.
EF.INC-CSQ	
Description	Un système de sauvegarde des Éléments essentiels et des données de l'organisation doit être mis en place. Il doit être testé une fois par mois et être réalisé avec des technologies de pointe. Ces mesures doivent être étudiées et mises en place par des experts du domaine. Elles doivent être testées au moins une fois par an.

6 - Administration de la sécurité

[Cette dernière section de l'énoncé des impératifs de sécurité concerne les moyens de garantir la continuité de la sécurité du système ou élu réseau informatique, une fois que celui-ci a reçu l'homologation, a été mis en exploitation et traite des informations classifiées, y compris les aspects liés au processus - initial et en cours - d'appréciation de la sécurité. Cette section doit aborder les aspects de gestion de la sécurité, y compris les rôles et responsabilités en matière de sécurité, les aspects de gestion des risques, le besoin de procédures d'exploitation de sécurité (SecOP), le contrôle de la configuration, les aspects de la maintenance liés à la sécurité, la documentation et la formation, les conditions de ré homologation du système ou du réseau informatique, et les dispositions relatives au retrait du système ou réseau informatique du service/à la liquidation de l'équipement.]