PREMIER MINISTRE
Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil

# Expression des Besoins et Identification des Objectifs de Sécurité

# EBIOS®

## ÉTUDE DE CAS @RCHIMED

Version du 16 juillet 2004

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 15 - Fax 01 71 75 84 00

Ce document a été réalisé par le bureau conseil de la DCSSI
(SGDN / DCSSI / SDO / BCS)
en collaboration avec le Club EBIOS

Les commentaires et suggestions sont encouragés et peuvent être adressés à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau Conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP

ebios.dcssi@sgdn.pm.gouv.fr

# Historique des modifications

| Date | Objet de la modification |
|---|---|
| 06/09/2000 | Création du document |
| 22/11/2000 | Restructuration du document<br>Remise en forme<br>Enrichissement du contenu |
| 29/10/2001 | Restructuration du document (regroupement des trois documents des versions précédentes en un)<br>Enrichissement du contenu (ajout d'explications)<br>Améliorations mineures (formulation des risques, modes d'exploitation, présentation des exercices et corrections) |
| 15/07/2002 | Améliorations des besoins et des objectifs de sécurité |
| 09/09/2003 | Convergence de l'étude de cas vers la nouvelle version de la méthode |
| 27/09/2003 | Améliorations suite à la formation pilote de septembre 2003 et en vue de la formation de formateurs d'octobre 2003 |
| 16/01/2004 | Mise en cohérence avec les dernières évolutions de la méthode, notamment les nouvelles bases de connaissances |
| 16/07/2004 | Intégration de la dernière version de l'étude de cas du logiciel. |

# Avertissement

**Le nom "*@rchimed*", donné à la société fictive dont il est question dans ce document, a été inventé et n'est utilisé que pour présenter une étude de cas du déroulement de la méthode EBIOS.**

# Table des matières

# 1 Introduction

Ce document présente une étude cas réalisée à l'aide la méthode EBIOS. Il est destiné à compléter la méthode dans le but d'apporter un exemple concret de son utilisation.

La première partie du document constitue le dossier de présentation de la société *@rchimed*. La suite décrit l'étude de sécurité. Toutes les étapes et activités seront présentées brièvement (en italique).

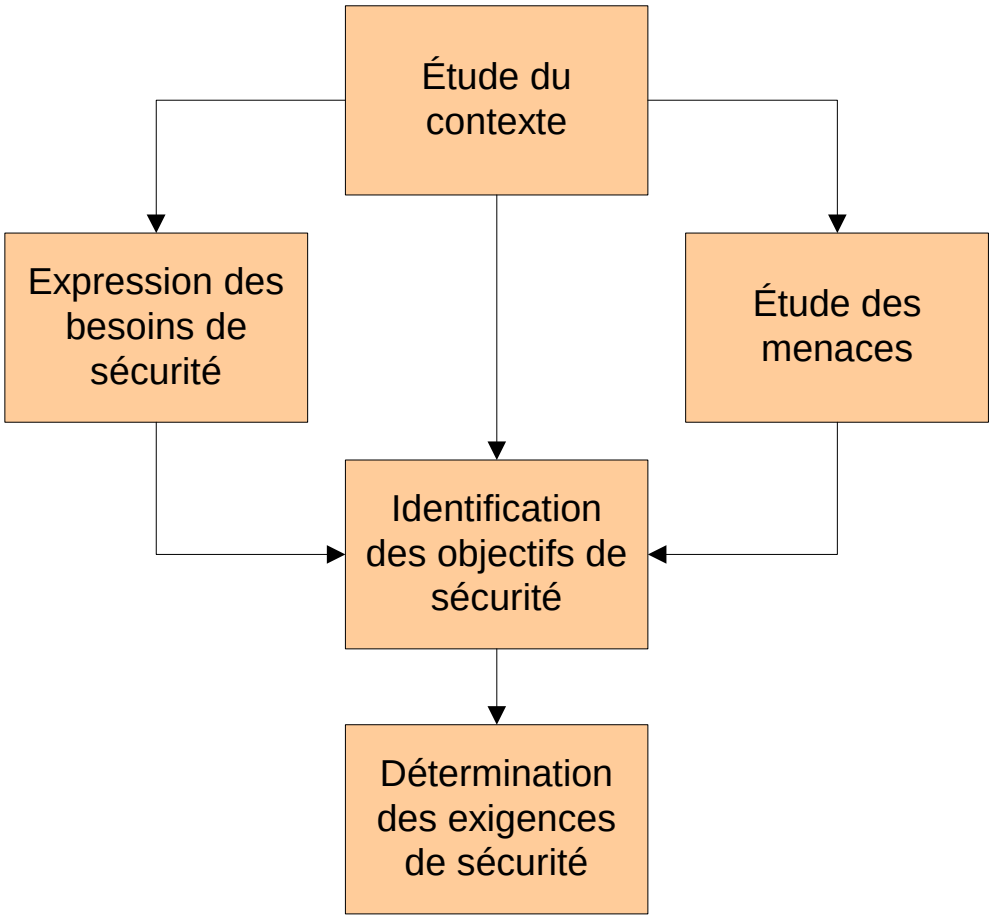



**Figure 1 - Étapes de la démarche EBIOS**

# 2 Dossier de présentation de la société *@rchimed*

Le dossier de présentation présente les informations relatives à la société *@rchimed*. Ces informations ont été rassemblées suite à un entretien avec les responsables de l'entreprise. Il sera bien sûr possible de recourir à de nouveaux entretiens ou de demander des informations complémentaires. **Il s'agit de réaliser l'étude EBIOS du système d'information de cette entreprise**.

## 2.1 Présentation générale de la société

La société *@rchimed* est un bureau d'ingénierie en architecture. Cette PME toulonnaise est constituée d'une douzaine de personnes. Son capital est de xxxxx € et son chiffre d'affaires est de yyyyy €.

## 2.2 Prestation fournie

La société *@rchimed* réalise des plans d'usines ou d'immeubles avec l'établissement du devis. Pour cela, elle calcule des structures, élabore des plans de visualisation pour les clients, et élabore des plans techniques pour les architectes. Le suivi des constructions est aussi assuré par le cabinet, qui met à jour les plans et calculs si des modifications sont nécessaires.

Le cabinet d'études commence à être réputé grâce à des solutions architecturales originales basées sur des techniques innovantes. Cette société concourt pour de grands projets nationaux ou internationaux ; elle s'appuie pour cela sur son système informatique qui lui permet de réagir extrêmement rapidement aux appels d'offre ou aux demandes des clients.

Elle attache également une importance extrême à la qualité des documents remis et plus précisément aux visualisations 3D qui permettent de donner aux clients une idée très précise de la solution proposée.

## 2.3 Structure de la société

### 2.3.1 Organigramme

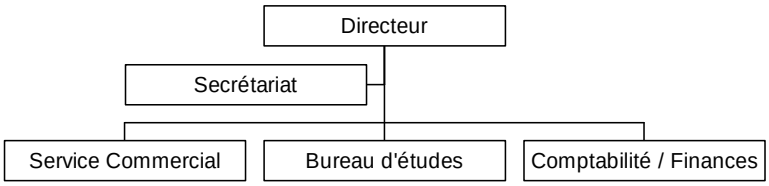



**Figure 2 - Organigramme de la société**

### 2.3.2 La direction

Elle est composée du directeur et de son adjoint. L'adjoint, bien qu'architecte de formation, fait office de "directeur informatique".

### 2.3.3 Le secrétariat

Il est animé par une secrétaire qui effectue également l'accueil téléphonique. Celle-ci dispose d'un micro-ordinateur équipé d'une suite bureautique - messagerie (connecté au serveur).

### 2.3.4 Le service commercial

Il est composé de deux personnes qui créent et gèrent les dossiers clients. Ils sont essentiellement chargés d'élaborer des devis pour les clients.

Seul, le service commercial est habilité à traiter avec l'extérieur, il est donc garant de l'image de marque de l'entreprise. Il échange fréquemment des informations avec le bureau d'études (plans,

visualisation des projets), avec la comptabilité (prix) et avec l'extérieur (cahier des charges, plans et devis avec les clients; éléments techniques avec les architectes ou les fournisseurs)

#### 2.3.5 Le bureau d'études

Il est composé de 4 ingénieurs et 3 techniciens supérieurs et réalise les activités suivantes :
- élabore des plans d'exécution destinés aux professionnels ;
- élabore des visualisations de projet sous une forme la plus séduisante possible destinés aux clients ;
- établit des calculs de résistances de structures et de matériaux.

#### 2.3.6 Le service comptabilité / finances

Le service chargé de toute la comptabilité est composé d'une seule personne. Il traite notamment avec la DDE pour les acceptations de permis de construire et s'occupe également de tous les contentieux.

## 2.4 Clientèle

Cette entreprise compte de nombreux clients, privés ou appartenant à l'administration, ainsi que les professionnels du bâtiment.

Les différentes statistiques menées depuis 3 ans montrent d'une part que les périodes de pointe se situent entre octobre et mai, et que la conjoncture générale est bonne.

Dans un contexte de rude concurrence, rapidité, précision et originalité des travaux sont des composantes essentielles de son activité.

## 2.5 Structure informatique

#### 2.5.1 Matériel

Toute l'informatique est reliée par un réseau interne fermé de type Ethernet. Le bureau d'étude possède 7 ordinateurs, le service commercial 2 ordinateurs, le service comptabilité/finances 1 ordinateur et le secrétariat 1 ordinateur. Tous ces ordinateurs sont de type PC. Le service commercial dispose de plus d'ordinateurs portables.

#### 2.5.2 Logiciels

Le cabinet a acquis le logiciel ARC+ pour la visualisation, le logiciel SIFRA pour le travail à partir de la tablette, et le logiciel SPOT pour les calculs de résistance des matériaux. Celui-ci comprend des données de base et les données résultats. Cet investissement a représenté un gros effort financier de la part de l'entreprise (plus de 3MF). La bureautique peut être traitée sur ces postes à partir des logiciels installés sur le serveur. L'outil de PAO (Pagemaker) est compatible avec les outils de CAO. Le système d'exploitation est Windows® NT. L'outil de visualisation permet de donner aux projets un aspect de photo réaliste.

## 2.6 Sécurité

#### 2.6.1 Sécurité du système d'information

Il n'y a pas de principes généraux, ni de politique de sécurité, seulement quelques règles :
- le contrôle d'accès se fait par identifiant /mot de passe ;
- principe de sauvegarde de tout fichier ;
- chaque ingénieur est responsable du fichier qu'il traite, les fichiers sont sauvegardés sur des disquettes stockées dans une armoire fermant à clé, située dans le bureau d'études ;
- parallèlement, les documents papiers sont rangés dans une armoire forte du service commercial ;

® Windows est une marque ou une marque déposée de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

- en ce qui concerne la maintenance, un contrat a été établi avec les fournisseurs de logiciels avec intervention sous 4 heures.

### 2.6.2 Sécurité générale

Nous avons pu recueillir les informations suivantes :
- les moyens réglementaires de lutte contre l'incendie sont en place ;
- il existe des consignes de fermeture à clé des locaux, mais aucun moyen, ni procédure de contrôle n'ont été mis en place ;
- le bureau d'études et le service commercial sont climatisés ;
- une alarme anti-intrusion est active durant les heures de fermeture (19h-7h), de fréquentes rondes de police ont lieu en ville ;
- le service de nettoyage intervient de 7h à 8h ;
- la direction est située au premier étage d'un immeuble qui se trouve en centre-ville ; différents commerces constituent son voisinage ; le bureau d'études et le service commercial sont au rez-de-chaussée ;
- le bureau du directeur est le seul à bénéficier d'une clé de sécurité qu'il détient ;
- les clients sont reçus dans le bureau des commerciaux, mais il arrive que des visites aient lieu au bureau d'études (pour démonstration) ;
- le serveur central situé dans une pièce isolée, contiguë au bureau d'études bénéficie d'une alimentation secourue ; c'est dans cette pièce que sont également disposées les imprimantes.

## 2.7 Contexte

La mise en réseau du système informatique s'est effectuée avec succès et a permis de réduire encore plus les délais de réalisation des travaux.

L'entreprise doit maintenant répondre au souhait de la majorité des clients qui est de correspondre directement avec le bureau d'étude via Internet pour transmettre tous les types de documents (dossiers techniques, devis, appel d'offre, messages...).

D'autre part, un important contrat avec une société est conditionné par la capacité du cabinet à assurer la confidentialité relative aux aspects techniques du projet.

L'entreprise a dernièrement perdu un marché : la rénovation de la mairie de Draguignan. Lors de la présentation des projets, il est apparu de curieuses similitudes entre la maquette d'*@rchimed* et celle d'un concurrent de Nice. Le directeur d'*@rchimed* soupçonne une compromission du projet qu'il avait présenté. Il a maintenant des craintes sur la confidentialité de certains projets.

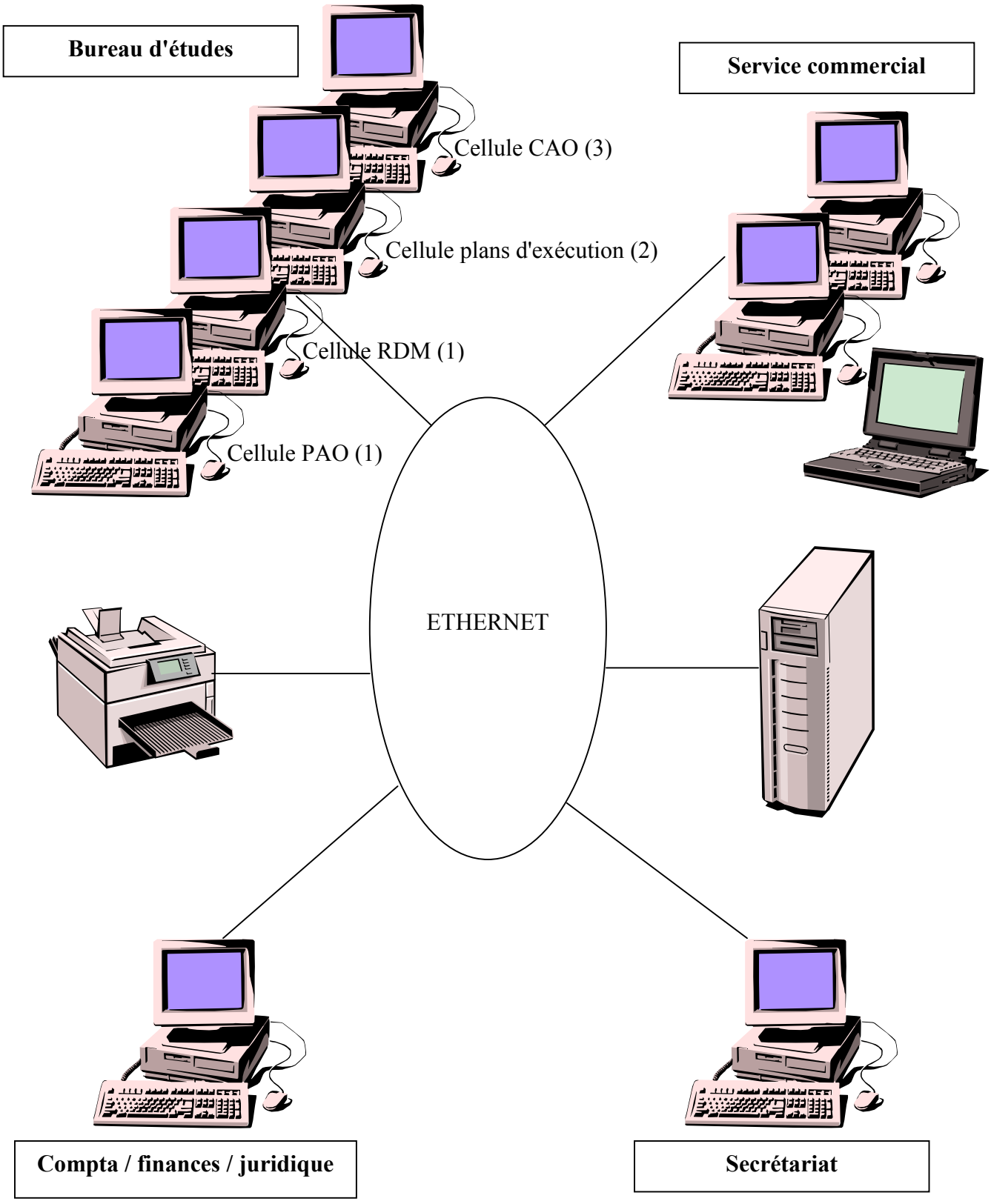
**L'arsenal de Toulon semble vouloir rénover certaines installations servant à la maintenance des bâtiments de la marine nationale. *@rchimed* souhaiterait pouvoir se présenter à d'éventuels appels d'offres.**

Compte tenu de son volume et de sa disposition, la société travaille de façon très ouverte. Cependant, les experts du bureau d'études sont les seuls à pouvoir accéder aux logiciels les plus performants de conception et de visualisation. Ces experts ont par ailleurs bénéficié d'une formation à la manipulation de ces outils.

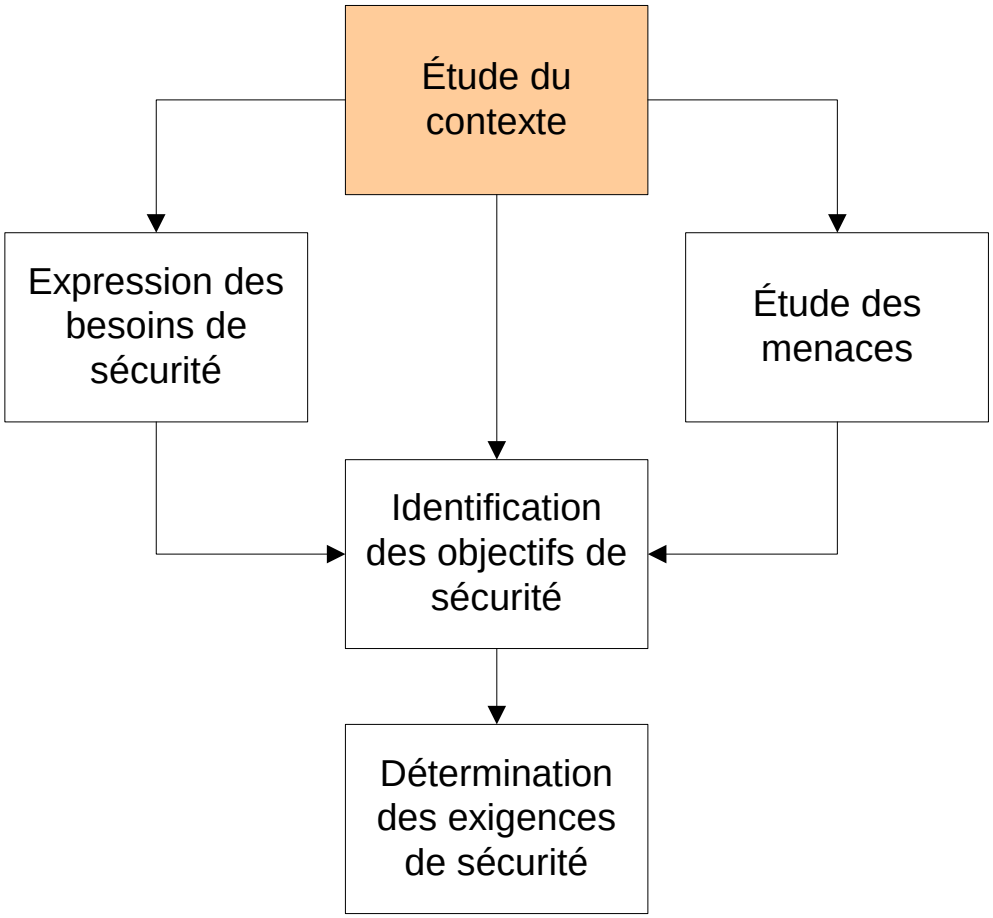
Chacun est conscient de ces responsabilités financières, civiles et pénales associées à l'usage des informations qu'il manipule : dossier client, données nominatives…

Le choix d'une étude de sécurité s'impose donc pour, d'une part, déterminer les conditions qui permettent l'ouverture du système informatique vers l'extérieur et d'autre part pour déterminer les mesures de sécurité nécessaires à la protection des projets sensibles.

## 2.8 Schéma du système informatique



# 3 Étape 1 : Étude du contexte




*Étape essentielle à toute démarche, la première partie du travail consiste à définir et délimiter l'étude. Pour cela, nous présentons tout d'abord le contexte général, c'est-à-dire l'organisme demandeur. Nous centrons ensuite l'étude sur le système-cible que nous allons définir. Pour terminer, nous nous intéressons à la cible précise de l'étude dont nous déterminons les différents éléments.*

*Nous réalisons cette première partie à l'aide d'un recueil de documents de l'organisme, de divers entretiens ou de questionnaires.*

## 3.1 Activité 1.1 : Étude de l'organisme

*Pour commencer, nous définissons le cadre de notre étude. Nous réunissons donc des informations générales sur l'organisme en question, dans le but de mieux apprécier sa nature, son organisation et les contraintes qui pèsent sur celui-ci.*

*Les contraintes seront à prendre en compte tout au long de la démarche, afin de garantir la cohérence avec le contexte.*

*D'une manière générale, les exigences réglementaires peuvent être considérées comme des règles de sécurité, dans la mesure où l'organisme souhaite les respecter.*

### 3.1.1 Présentation de l'organisme

| Organisme | |
|---|---|
| Présentation | Nom de l'organisme : @RCHIMED<br><br>Capital : xxxxx euros<br><br>CA : yyyyy euros<br><br>Présentation : Il s'agit d'une PME toulonnaise constituée d'une douzaine de personnes. C'est un bureau d'ingénierie en architecture qui réalise des plans d'usines et d'immeubles.<br><br>Vocation principale : Société de services pour les professionnels du bâtiment.<br><br>Métier :<br>- Architecture<br>- Ingénierie du bâtiment<br><br>Missions :<br>- Élaboration de projets architecturaux<br>- Élaboration des calculs et plans de réalisation<br><br>Valeurs propres :<br>- Réactivité<br>- Précision des travaux<br>- Créativité architecturale<br>- Communication<br><br>Structure de l'organisme : Fonctionnelle<br><br>Axes stratégiques :<br>- Utilisation des nouvelles technologies (Internet, Intranet) dans un but d'ouverture vers l'extérieur et d'optimisation des moyens<br>- Consolidation de l'image de marque (protection des projets sensibles) |

### 3.1.2 Contraintes pesant sur l'organisme

| C.CONCURRENCE | |
|---|---|
| Thème | Contraintes conjoncturelles |
| Description | Secteur de rude concurrence |
| **C.APPELS-OFFRES** | |

| | |
|---|---|
| Thème | Contraintes conjoncturelles |
| Description | Dépendance des appels d'offres |

| C.CRISE | |
|---|---|
| Thème | Contraintes conjoncturelles |
| Description | Seule une crise très grave dans le bâtiment pourrait affecter le fonctionnement du cabinet d'études |

| C.UTILISATEUR | |
|---|---|
| Thème | Contraintes relatives au personnel |
| Description | Le personnel est utilisateur de l'informatique, mais pas spécialiste |

| C.RESPONSABLE | |
|---|---|
| Thème | Contraintes relatives au personnel |
| Description | Le responsable informatique est l'adjoint du directeur, il est architecte de formation |

| C.NETTOYAGE | |
|---|---|
| Thème | Contraintes relatives au personnel |
| Description | Le personnel de nettoyage intervient de 7h à 8h |

| C.CLIENTS | |
|---|---|
| Thème | Contraintes relatives au personnel |
| Description | La réception des clients se fait dans les bureaux des commerciaux, mais des visites ont parfois lieu au bureau d'études |

| C.POINTE | |
|---|---|
| Thème | Contraintes d'ordre calendaire |
| Description | La période de pointe se situant d'octobre à mai, toute action (installation de système de sécurité, formation et sensibilisation) se fera en dehors de cette période |

| C.INVESTISSEMENT | |
|---|---|
| Thème | Contraintes d'ordre budgétaire |
| Description | La société a fait un effort important en matière d'informatisation, tout investissement supplémentaire devra être dûment justifié |

| C.ARCHITECTURE | |
|---|---|
| Thème | Contraintes d'ordre technique |
| Description | Respect des règles de conception architecturale |

| C.LOGICIELS | |
|---|---|
| Thème | Contraintes d'ordre technique |
| Description | Utilisation des logiciels professionnels du domaine architectural |

| C.IMMEUBLE | |
|---|---|
| Thème | Contraintes d'environnement |
| Description | Le cabinet loue deux étages d'un immeuble au centre ville |

| C.COMMERCES | |
|---|---|
| Thème | Contraintes d'environnement |
| Description | Voisinage de commerces divers |

| C.DEMENAGEMENT | |
|---|---|
| Thème | Contraintes d'environnement |

| | |
|---|---|
| Description | Aucun déménagement n'est planifié |
| **C.CONFIDENTIALITE** | |
| Thème | Contraintes d'ordre stratégique |
| Description | L'entreprise devra déterminer les mesures de sécurités nécessaires à la protection de projets sensibles |

### 3.1.3 Références réglementaires applicables à l'organisme

| | |
|---|---|
| **P.901** | |
| Libellé étendu | Recommandation n°901 |
| Description | Recommandation pour la protection des systèmes d'information traitant des informations sensibles non classifiées de défense. |
| **P.CNIL** | |
| Libellé étendu | Loi n°78-17 du 6 janvier 1978 - Informatique et libertés |
| Description | Loi relative à l'informatique, aux fichiers et aux libertés |
| **P.DDE** | |
| Libellé étendu | Règlement DDE |
| Description | Prise en compte de l'environnement, respect des règles architecturales, permis de construire... |
| **P.MARCHES** | |
| Libellé étendu | Code des marchés publics |
| Description | |

### 3.1.4 Description fonctionnelle du système d'information global

| | | |
|---|---|---|
| Domaines d'activité | **Gestion administrative** | |
| | Définition | Gestion administrative (comptabilité, finances, juridique...) :<br>- Gérer la comptabilité<br>- Gérer les contentieux juridiques et techniques<br>- Gérer les permis de construire<br>- Gérer les ressources humaines<br>- Gérer les fournitures et la maintenance<br>- Gérer les assurances |
| | Liaisons | Autres organismes<br>Client<br>Gestion des relations commerciales |
| | **Gestion des relations commerciales** | |
| | Définition | Gestion des relations commerciales (service commercial) :<br>- Établir les devis<br>- Gérer les projets |

| | |
|---|---|
| Liaisons | Cotraitant bâtiment<br>Client<br>Gestion des études<br>Gestion administrative |

**Gestion des études**

| | |
|---|---|
| Définition | Gestion des études (bureau d'études) :<br>- Créer des visualisations<br>- Calculer les structures<br>- Créer des plans techniques |
| Liaisons | Cotraitant informatique<br>Gestion des relations commerciales |

Acteurs externes

**Client**

| | |
|---|---|
| Nom | Client |
| Titre | Client |
| Description | Cette entreprise compte de nombreux clients, privés ou appartenant à l'administration, ainsi que les professionnels du bâtiment |
| Liaisons | Gestion administrative<br>Gestion des relations commerciales |

**Cotraitant bâtiment**

| | |
|---|---|
| Nom | Cotraitant bâtiment |
| Titre | Cotraitant bâtiment |
| Description | Cotraitant bâtiment (fournisseurs, professionnels du bâtiment ...) |
| Liaisons | Gestion des relations commerciales |

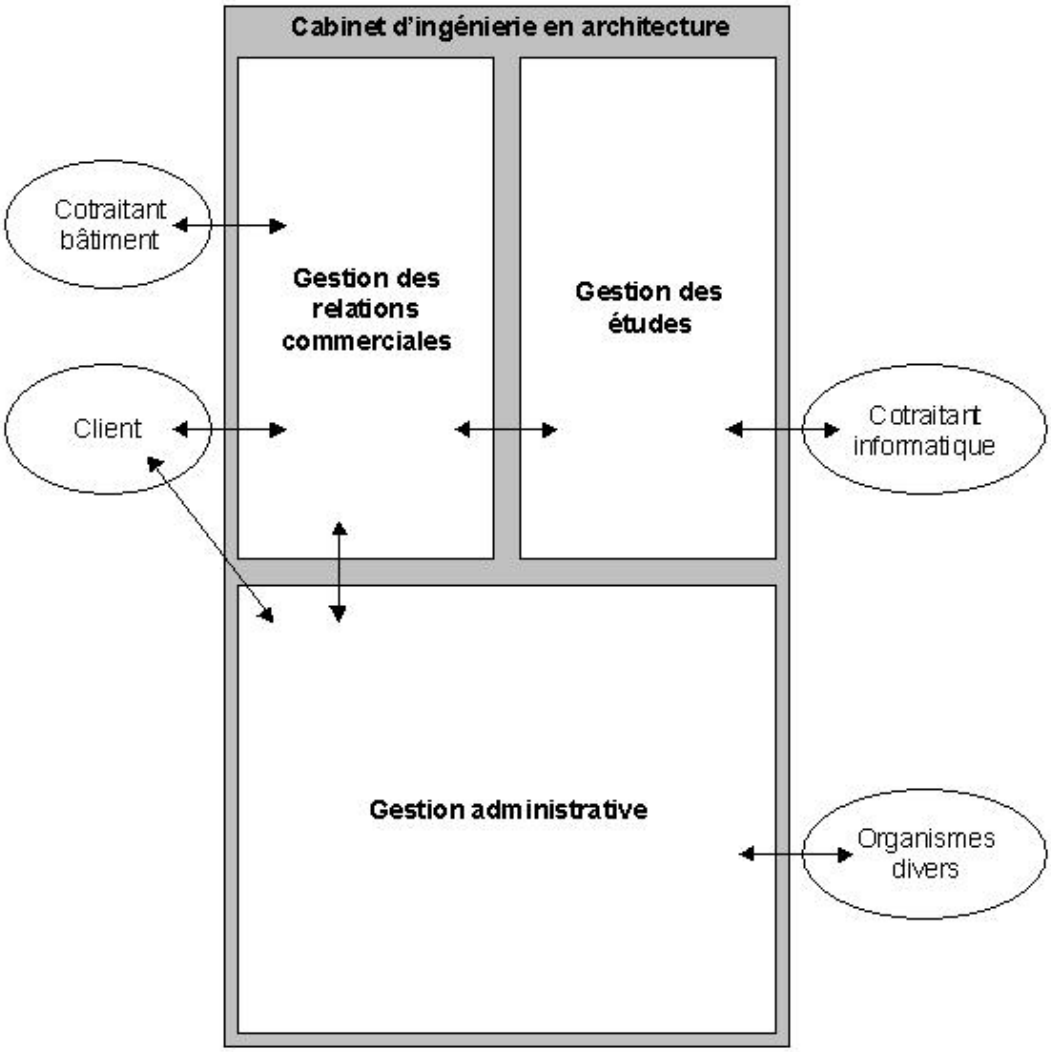
**Cotraitant informatique**

| | |
|---|---|
| Nom | Cotraitant informatique |
| Titre | Cotraitant informatique |
| Description | Cotraitant informatique (mises à jour des paramètres techniques) |
| Liaisons | Gestion des études |

**Autres organismes**

| | |
|---|---|
| Nom | Autres organismes |
| Titre | Autres organismes |
| Description | Autres organismes (assurances, maintenance?) |
| Liaisons | Gestion administrative |

Schéma


Cabinet d'ingénierie en architecture
Cotraitant bâtiment
Gestion des relations commerciales
Gestion des études
Client
Cotraitant informatique
Gestion administrative
Organismes divers

## 3.2 Activité 1.2 : Étude du système-cible

*Nous avons commencé par une étude globale de l'organisme. Nous nous intéressons maintenant à son système d'information, dont nous précisons le sous-ensemble constituant le système-cible de l'étude et ses enjeux.*

*D'une manière générale, les enjeux du système-cible peuvent être considérés comme des hypothèses.*

### 3.2.1 Présentation du système-cible

| Système-cible | |
|---|---|
| Présentation | Le métier de la société correspond à la majeure partie du système d'information. Le système-cible correspond donc à un sous-ensemble de celui-ci qui concerne le métier du cabinet d'études.<br><br>Nous écartons par conséquent :<br>- la partie gestion administrative interne (ressources humaines, maintenance, assurances),<br>- la gestion des permis de construire.<br><br>Le système-cible est le suivant :<br>- gestion des relations commerciales :<br>  - établir les devis,<br>  - gérer les projets ;<br>- gestion des études :<br>  - calculer les structures,<br>  - créer des plans techniques,<br>  - créer des visualisations ;<br>- une partie de la gestion administrative :<br>  - gérer la comptabilité,<br>  - gérer les contentieux juridiques et techniques. |

### 3.2.2 Enjeux du système-cible

| H.REORGANISATION | |
|---|---|
| Description | L'entreprise veut augmenter les capacités de son bureau d'études, le système-cible est donc au cœur des priorités, puisqu'il constitue son outil principal. L'analyse des risques SSI est donc directement en lien avec la vie du cabinet d'études. |

| H.INFORMATIQUE | |
|---|---|
| Description | Aujourd'hui, le cabinet d'études ne dispose pas réellement de compétences dans le domaine informatique, cependant, compte tenu de son ouverture vers l'extérieur et des enjeux fonctionnels et de sécurité concomitants, il sera nécessaire de coupler les réflexions sur l'organisation du travail et des services avec celles sur l'informatique. |

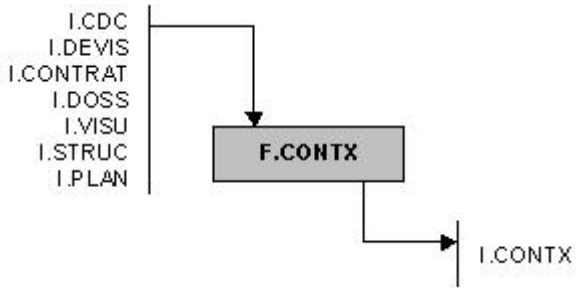
| H.SERVICES | |
|---|---|
| Description | Le cabinet d'études a identifié dans sa stratégie commerciale la nécessité d'améliorer les services rendus aux usagers et la qualité des prestations. |

| H.ECHANGES | |
|---|---|
| Description | Le cabinet d'études a identifié dans sa stratégie commerciale la nécessité |

| | |
|---|---|
| | architectes). |
| **H.METIERS** | |
| Description | Le cabinet d'études a identifié dans sa stratégie ce développement la nécessité de contribuer aux évolutions des structures et des métiers. |

### 3.2.3 Liste des éléments essentiels

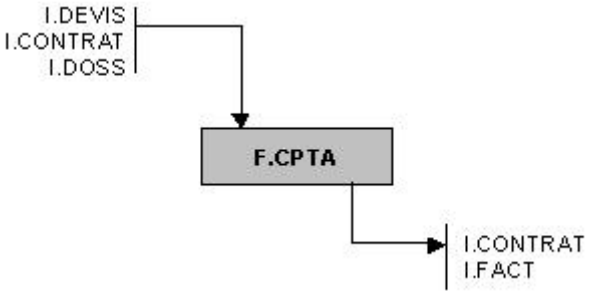
| | |
|---|---|
| **Information : I.CDC** | |
| Description | Cahier des charges |
| **Information : I.CONTRAT** | |
| Description | Contrat (demande de réalisation) |
| **Information : I.CONTX** | |
| Description | Dossier de contentieux |
| **Information : I.DEVIS** | |
| Description | Devis |
| **Information : I.DOSS** | |
| Description | Dossier technique d'un projet |
| **Information : I.FACT** | |
| Description | Facture |
| **Information : I.PARA** | |
| Description | Paramètres techniques (pour les calculs de structure) |
| **Information : I.PLAN** | |
| Description | Plan technique |
| **Information : I.STRUC** | |
| Description | Résultat de calcul de structure |
| **Information : I.TECH** | |
| Description | Catalogues techniques |
| **Information : I.VISU** | |
| Description | Visualisation |

| | |
|---|---|
| **Fonction : F.CONTX** | |
| Schéma |  |
| Description | Gérer les contentieux juridiques et techniques |
| Entrées | |

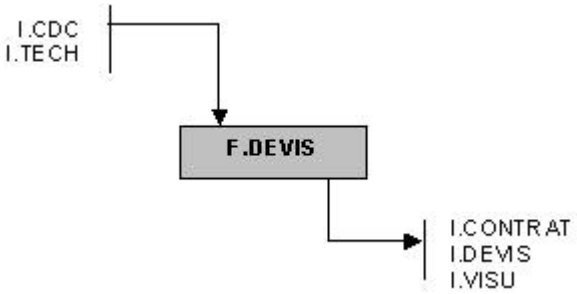
I.PLAN

| | |
|---|---|
| | I.PLAN<br>I.DOSS<br>I.DEVIS<br>I.CONTRAT<br>I.CDC |
| Sorties | I.CONTX |

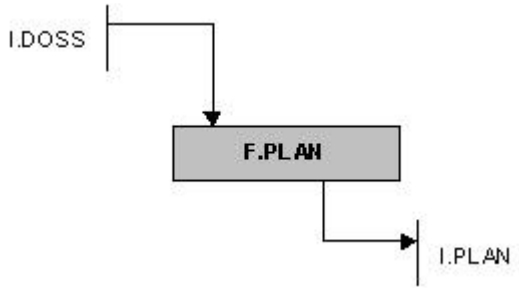
**Fonction : F.CPTA**

| | |
|---|---|
| Schéma |  |
| Description | Gérer la comptabilité |
| Entrées | I.DOSS<br>I.DEVIS<br>I.CONTRAT |
| Sorties | I.FACT<br>I.CONTRAT |

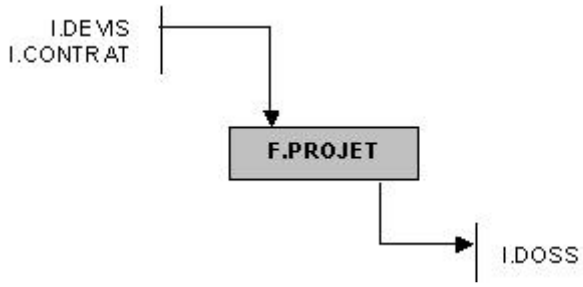
**Fonction : F.DEVIS**

| | |
|---|---|
| Schéma |  |
| Description | Établir les devis (estimation du coût global d'un projet, négociations avec les clients autour de maquettes virtuelles en trois dimensions) |
| Entrées | I.TECH<br>I.CDC |
| Sorties | I.VISU<br>I.DEVIS<br>I.CONTRAT |

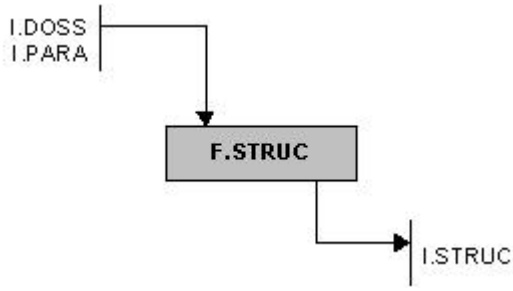
## Fonction : F.PLAN

| | |
|---|---|
| Schéma |  |
| Description | Créer des plans techniques |
| Entrées | I.DOSS |
| Sorties | I.PLAN |

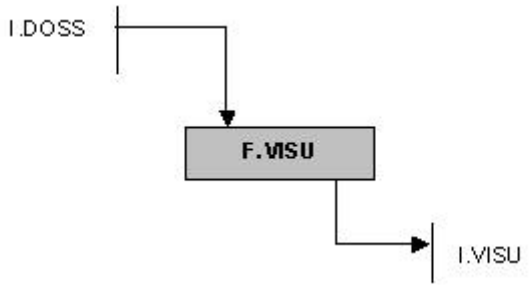
## Fonction : F.PROJET

| | |
|---|---|
| Schéma |  |
| Description | Gérer les projets |
| Entrées | I.DEVIS<br>I.CONTRAT |
| Sorties | I.DOSS |

## Fonction : F.STRUC

| | |
|---|---|
| Schéma |  |
| Description | Calculer les structures |
| Entrées | I.PARA<br>I.DOSS |
| Sorties | I.STRUC |

**Fonction : F.VISU**

| | |
|---|---|
| Schéma |  |
| Description | Créer des visualisations |
| Entrées | I.DOSS |
| Sorties | I.VISU |

### 3.2.4 Liste des contraintes spécifiques pesant sur le système-cible

| C.CLIMATISATION | |
|---|---|
| Thème | Contraintes d'environnement |
| Description | Le bureau d'études et le service commercial sont climatisés |

### 3.2.5 Liste des références réglementaires spécifiques

Aucune référence réglementaire spécifique.

### 3.2.6 Liste des hypothèses

| H.USAGE | |
|---|---|
| Description | Les utilisateurs du système d'information d'@rchimed ont connaissance des valeurs et des axes stratégiques exprimés par le directeur. En particulier, l'innovation et la réactivité sont des valeurs partagées. Dans ce contexte, chacun sait la valeur que représentent les logiciels de conception. |

| H.LOI | |
|---|---|
| Description | Chacun au sein de la société connaît ses responsabilités en cas de diffusion illicite d'informations métiers ou de manipulation illégale de données nominatives. |

| H.POLICE | |
|---|---|
| Description | De fréquentes rondes de police ont lieu en ville |

*Nous déterminons aussi un mode d'exploitation de sécurité parmi trois modes possibles :*

- *le mode exclusif ;*
  ***Toutes** les personnes ayant accès au système sont habilitées au plus haut niveau de classification et elles possèdent un besoin commun d'en connaître (ou équivalent) pour **toutes** les informations traitées, stockées ou transmises par le système.*
- *le mode dominant ;*
  ***Toutes** les personnes ayant accès au système sont habilitées au plus haut niveau de classification mais elles n'ont **pas toutes** un besoin commun d'en connaître (ou équivalent) pour les informations traitées, stockées ou transmises par le système.*
- *le mode multi-niveaux.*
  *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.*

*Ce choix s'effectue en fonction des informations manipulées, des niveaux d'habilitations des utilisateurs et du besoin d'en connaître. Dans la majorité des cas, les systèmes d'information fonctionnent selon un mode dominant.*
*Le mode d'exploitation peut être considéré comme une hypothèse.*

| H.DOMINANT | |
|---|---|
| Niveau | 2 |
| Description | Le mode d'exploitation du système est du type dominant.<br><br>Toutes les personnes ayant accès au système sont habilitées au plus haut niveau de classification mais elles n'ont pas toutes un besoin commun d'en connaître (ou équivalent) pour les informations traitées, stockées ou transmises par le système. |

### 3.2.7 Liste des règles de sécurité

| | |
|---|---|
| **P.ALARME** | |
| Description | Une alarme anti-intrusion est active durant les heures de fermeture (19h-7h) |
| **P.ARMOIRE-DISQ** | |
| Description | Les fichiers sont sauvegardés sur des disquettes stockées dans une armoire fermant à clé, située dans le bureau d'étude |
| **P.ARMOIRE-DOC** | |
| Description | Les documents papiers sont rangés dans une armoire forte du service commercial |
| **P.INCENDIE** | |
| Description | Moyens réglementaires de lutte contre l'incendie mis en place |
| **P.INCENDIE-PLAN** | |
| Description | Plan de sécurité incendie |
| **P.RESP-FICHIER** | |
| Description | Chaque ingénieur est responsable du fichier qu'il traite |
| **P.SAUVEGARDE** | |
| Description | Principe de sauvegarde de tout fichier |
| **P.CONTROLE-ACCES** | |
| Description | Le contrôle d'accès se fait au moins par identifiant / mot de passe |
| **P.FERMETURE** | |
| Description | Consigne de fermeture à clé des bureaux en cas d'absence |

## 3.3 Activité 1.3 : Détermination de la cible de l'étude de sécurité

*Nous déterminons enfin les entités qui composent la cible. De cette manière, il est possible d'élaborer les tableaux de relations fonctions / entités et informations / entités avec les fonctions et informations essentielles retenues précédemment.*

### 3.3.1 Liste des entités du système

| | |
|---|---|
| **E.ADSL** | |
| Type | RES_INF : Médium et supports |
| Description | Ligne asymétrique numérique se trouvant entre le modem ADSL installé chez l'abonné et le central téléphonique |
| **E.ARC+** | |
| Type | LOG_APP.1 : Application métier standard |
| Description | ARC+ (visualisation) |
| **E.BUR** | |
| Type | MAT_ACT.2 : Matériel fixe |
| Description | Ordinateur bureautique |
| **E.CAO** | |
| Type | MAT_ACT.2 : Matériel fixe |
| Description | Ordinateur CAO |
| **E.COMM** | |
| Type | PER_UTI : Utilisateurs |
| Description | Commercial |
| **E.CPTA** | |
| Type | PER_UTI : Utilisateurs |
| Description | Comptable |
| **E.CRM** | |
| Type | MAT_ACT.2 : Matériel fixe |
| Description | Ordinateur Calcul de Résistance des Matériaux |
| **E.DIR** | |
| Type | PER_DEC : Décisionnel |
| Description | Directeur |
| **E.EDF** | |
| Type | PHY_SRV.2 : Énergie |
| Description | Fournisseur de réseau électrique |
| **E.ETH** | |
| Type | RES_INF : Médium et supports |
| Description | Réseau local Ethernet entre toutes les machines |
| **E.EXP** | |
| Type | PER_EXP : Exploitant / Maintenance |
| Description | Directeur informatique (directeur adjoint) |

| **E.FSI** | |
|---|---|
| Type | PHY_SRV.1 : Communication |
| Description | Fournisseur de services Internet (WANADOO, CLUB-INTERNET, AOL, LYBERTYSURF, NET-UP, TISCALI...) |

| **E.IMPR** | |
|---|---|
| Type | MAT_ACT.3 : Périphérique de traitement |
| Description | Imprimante connectée au réseau |

| **E.ING** | |
|---|---|
| Type | PER_UTI : Utilisateurs |
| Description | Ingénieur |

| **E.MAGN** | |
|---|---|
| Type | MAT_PAS.1 : Support électronique |
| Description | Supports magnétiques |

| **E.MESS** | |
|---|---|
| Type | LOG_STD : Progiciel ou logiciel standard |
| Description | Outil de messagerie |

| **E.OFFI** | |
|---|---|
| Type | LOG_STD : Progiciel ou logiciel standard |
| Description | Suite bureautique |

| **E.ORGA** | |
|---|---|
| Type | ORG_GEN : Organisation de l'organisme |
| Description | Organisation du cabinet d'études |

| **E.PAO** | |
|---|---|
| Type | MAT_ACT.2 : Matériel fixe |
| Description | Ordinateur PAO |

| **E.PAP** | |
|---|---|
| Type | MAT_PAS.2 : Autres supports |
| Description | Support papiers |

| **E.PGMK** | |
|---|---|
| Type | LOG_STD : Progiciel ou logiciel standard |
| Description | Pagemaker (PAO) |

| **E.PLAN** | |
|---|---|
| Type | MAT_ACT.2 : Matériel fixe |
| Description | Ordinateur Plans d'exécution |

| **E.PORTABLE** | |
|---|---|
| Type | MAT_ACT.1 : Matériel transportable |
| Description | Ordinateur portable du service commercial |

| **E.SECR** | |
|---|---|
| Type | PER_UTI : Utilisateurs |
| Description | Secrétaire |

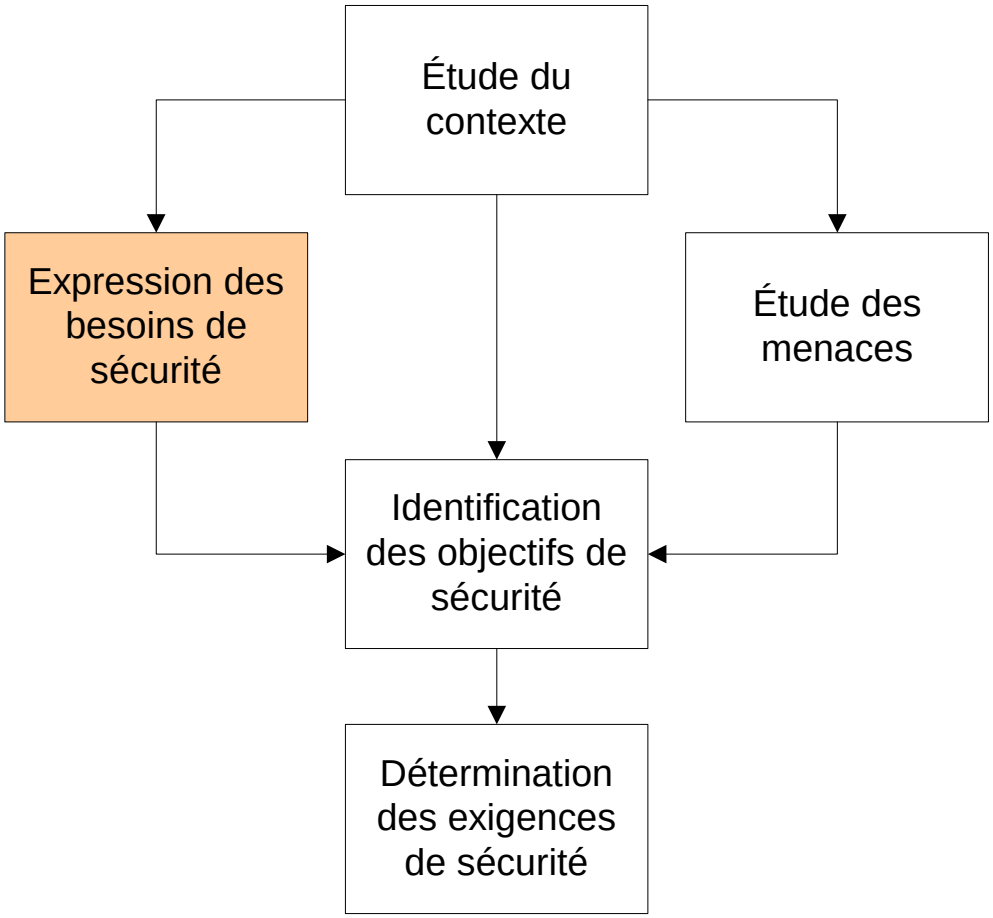
| **E.SERV** | |
|---|---|
| Type | MAT_ACT.2 : Matériel fixe |
| Description | Serveur de réseau, messagerie et bureautique |
| **E.SIFRA** | |
| Type | LOG_APP.1 : Application métier standard |
| Description | SIFRA (tablette à digitaliser) |
| **E.SITE** | |
| Type | PHY_LIE.2 : Locaux |
| Description | Site du cabinet d'études |
| **E.SPOT** | |
| Type | LOG_APP.1 : Application métier standard |
| Description | SPOT (calculs de résistance) |
| **E.TECH** | |
| Type | PER_UTI : Utilisateurs |
| Description | Technicien |
| **E.TEL** | |
| Type | PHY_SRV.1 : Communication |
| Description | Ligne téléphonique |
| **E.WNT** | |
| Type | LOG_OS : Système d'exploitation |
| Description | Windows® NT (système d'exploitation) |

® Windows est une marque ou une marque déposée de Microsoft Corporation aux États-Unis et/ou dans d'autres pays.

### 3.3.2 Réalisation des tableaux entités / éléments essentiels

| | E.ARC+ | E.SIFRA | E.SPOT | E.WNT | E.MESS | E.OFFI | E.PGMK | E.PORTA | E.BUR | E.CAO | E.CRM | E.PAO | E.PLAN | E.SERV | E.IMPR | E.MAGN | E.PAP | E.ORGA | E.DIR | E.EXP | E.COMM | E.CPTA | E.ING | E.SECR | E.TECH | E.SITE | E.FSI | E.TEL | E.EDF | E.ADSL | E.ETH |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| F.CONTX | | | | X | X | X | | | X | | | | | X | X | | X | X | X | X | X | X | X | | X | X | X | X | X | X | X |
| F.CPTA | | | | X | X | X | | | X | | | | | X | X | X | X | X | X | X | X | X | | X | | X | X | X | X | X | X |
| F.DEVIS | | | | X | X | X | | X | X | | | | | X | X | | X | X | X | X | X | | X | | X | X | X | X | X | X | X |
| F.PLAN | | X | | X | X | | X | | | | | X | X | X | X | X | X | X | X | X | X | | X | | X | X | X | | X | X | X |
| F.PROJET | | | | X | X | X | | | X | | | | | X | X | | X | X | X | X | X | | X | X | X | X | X | X | X | X | X |
| F.STRUC | | | X | X | X | | X | | | | X | X | | X | X | X | X | X | X | X | X | | X | | X | X | X | | X | X | X |
| F.VISU | X | | | X | X | | X | | | X | | X | | X | X | X | X | X | X | X | X | | X | | X | X | X | | X | X | X |
| I.CDC | | | | X | X | X | | X | X | | | | | X | X | X | X | X | X | X | X | | X | | X | X | X | X | X | X | X |
| I.CONTRAT | | | | X | X | X | | X | X | | | | | X | X | X | X | X | X | X | | X | X | X | | X | X | X | X | X | X |
| I.CONTX | | | | X | X | X | | | X | | | | | X | X | X | X | X | X | X | X | X | X | | | X | X | X | X | X | X |
| I.DEVIS | | | | X | X | X | | X | X | | | | | X | X | X | X | X | X | X | X | | X | X | | X | X | X | X | X | X |
| I.DOSS | | | | X | X | X | | | X | | | | | X | X | X | X | X | X | X | | | X | X | X | X | X | X | X | X | X |
| I.FACT | | | | X | X | X | | | X | | | | | X | X | X | X | X | X | X | | X | X | | | X | X | X | X | X | X |
| I.PARA | | | | X | X | X | | | | | | | | X | X | X | X | X | X | X | | | X | | X | X | X | | X | X | X |
| I.PLAN | | X | | X | X | X | X | X | X | | | X | X | X | X | X | X | X | X | X | | | X | | X | X | X | | X | X | X |
| I.STRUC | | | X | X | X | | X | | | | X | X | | X | X | X | X | X | X | X | | | X | | X | X | X | | X | X | X |
| I.TECH | | | | X | X | | | | | | | | | X | X | X | X | X | X | X | X | | X | | | X | X | X | X | X | X |
| I.VISU | X | | | X | X | | X | X | | X | | X | | X | X | X | X | X | X | X | | | X | | | X | X | | X | X | X |

# 4 Étape 2 : Expression des besoins de sécurité




*La cible de l'étude étant identifiée, nous allons maintenant exprimer les besoins de sécurité de chacun des éléments essentiels, ainsi que le mode d'exploitation de sécurité du système.*

## 4.1 Activité 2.1 : Réalisation des fiches de besoins

*Afin de réaliser les fiches d'expression des besoins de sécurité, il est nécessaire de déterminer les critères de sécurité qui seront étudiés, une échelle de besoins explicite et objective, et des impacts explicites pour l'organisme. Ainsi, nous disposerons de tableaux d'expression des besoins de sécurité qui serviront pour chaque élément essentiel.*

### 4.1.1 Choix des critères de sécurité

*Il est nécessaire de choisir les **critères de sécurité** à prendre en compte. Les critères de sécurité couramment utilisés sont la disponibilité, l'intégrité et la confidentialité, mais il peut être pertinent d'en ajouter d'autres tels que la preuve, le contrôle, l'anonymat, la fiabilité… L'échelle de besoins sera déterminée en fonction de ces critères de sécurité.*

| **Confidentialité** | |
|---|---|
| Description | Propriété des éléments essentiels de n'être accessibles qu'aux utilisateurs autorisés.<br><br>Pour une fonction : protection des algorithmes décrivant les règles de gestion et les résultats dont la divulgation à un tiers non autorisé porterait préjudice ; absence de divulgation d'un traitement ou mécanisme à caractère confidentiel.<br><br>Pour une information : protection des données dont l'accès ou l'usage par des tiers non autorisés porterait préjudice ; absence de divulgation de données à caractère confidentiel. |
| **Disponibilité** | |
| Description | Propriété d'accessibilité au moment voulu des éléments essentiels par les utilisateurs autorisés.<br><br>Pour une fonction : garantie de la continuité des services de traitement ; absence de problèmes liés à des temps de réponse au sens large.<br><br>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. |
| **Intégrité** | |
| Description | Propriété d'exactitude et de complétude des éléments essentiels.<br><br>Pour une fonction : assurance de conformité de l'algorithme ou de la mise en œuvre des traitements automatisés ou non par rapport aux spécifications ; absence de résultats incorrects ou incomplets de la fonction.<br><br>Pour une information : garantie d'exactitude et d'exhaustivité des données vis-à-vis d'erreurs de manipulation ou d'usages non autorisés ; non-altération de l'information. |

### 4.1.2 Détermination de l'échelle de besoins

*Une graduation de ces critères de sécurité peut alors être élaborée. Pour cela, une **pondération** et des **valeurs de référence** doivent être déterminées pour chacun des critères de sécurité identifié.*

| | Confidentialité | Disponibilité | Intégrité |
|---|---|---|---|
| 0 | Public | Aucun besoin de disponibilité | Aucun besoin d'intégrité |
| | L'élément essentiel est accessible à tous sans aucune restriction. | L'élément essentiel peut être indisponible définitivement ou pas, sans que cela ait une conséquence. | Il n'y a aucun besoin de garantir l'intégrité de l'élément essentiel. |
| 1 | Restreint au cabinet et aux clients | Long terme | |
| | L'élément essentiel est accessible seulement pour une personne du cabinet d'études ou pour un client concerné et identifié. | L'élément essentiel peut être indisponible plus d'une semaine, mais il ne doit pas être perdu définitivement. | |
| 2 | Restreint au cabinet | Moyen terme | Besoin d'intégrité moyen |
| | L'élément essentiel est accessible seulement aux membres du cabinet d'études. | L'élément essentiel doit être disponible dans la semaine. | Besoin d'intégrité moyen |
| 3 | Confidentiel projet | Court terme | |
| | L'élément essentiel est accessible seulement aux personnes du cabinet d'études directement concernées par un projet défini. | L'élément essentiel doit être disponible dans la journée. | |
| 4 | Secret @rchimed | Très court terme (temps réel) | Parfaitement intègre |
| | L'élément essentiel est accessible seulement au président du cabinet d'études. | L'élément essentiel doit être disponible en temps réel. | L'élément essentiel doit être parfaitement intègre. |

### 4.1.3 Détermination des 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.*

*La méthode propose une liste d'impacts, dans laquelle nous ne garderons que les plus adéquats.*

*Afin de rendre les impacts plus objectifs, il convient de fournir des exemples explicites de chacun d'eux en termes de conséquences envisageables.*

*Nous avons alors tous les composants des fiches d'expression des besoins de sécurité.*

Ce sont principalement les valeurs, axes stratégiques et diverses contraintes pesant sur le cabinet d'études qui permettent de choisir des impacts pertinents.

| **Perte d'image de marque** | |
|---|---|
| Description | Exemples :<br>- perte de notoriété,<br>- mauvaise presse,<br>- bouche à oreille négatif,<br>- utilisation de la concurrence. |

| **Infraction aux lois, aux règlements** | |
|---|---|
| Description | Exemples :<br>- impossibilité de remplir les obligations légales,<br>- action en justice à l'encontre du cabinet,<br>- non respect de la réglementation métier. |

| **Perte d'un avantage concurrentiel** | |
|---|---|
| Description | Exemples :<br>- perte d'un savoir-faire métier,<br>- vol d'un savoir-faire métier. |

## 4.2 Activité 2.2 : Synthèse des besoins de sécurité

*Cette activité consiste à questionner des personnes de l'organisme afin de savoir quelle influence elles estiment qu'un sinistre donné a sur un impact donné. Ces personnes sont des utilisateurs du système et sont choisies par rapport aux fonctions ou informations qu'elles manipulent. Nous pouvons ainsi remplir les tableaux d'expression des besoins de sécurité et en élaborer une synthèse.*

### 4.2.1 Détermination des personnes à interroger

Nous retenons des types d'utilisateurs bien distincts pour le cabinet d'études, qui correspondent aux différents types de personnels rencontrés. Ceci nous permet d'interroger les personnes selon leur domaine de connaissances.

Types d'utilisateurs retenus :

- Ingénieur
- Technicien
- Commercial
- Comptable
- Secrétaire

### 4.2.2 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…).*

Exemple d'une fiche remplie par une personne pour un élément essentiel :

| **Ingénieur** | |
|---|---|
| Élément essentiel | F.DEVIS |
| Personne interrogée | Ingénieur |

Fiche d'expression des besoins de sécurité

| | | Perte d'image de marque | Infraction aux lois, aux règlements | Perte d'un avantage concurrentiel | Besoin de sécurité | Commentaires |
|---|---|---|---|---|---|---|
| Confidentialité | Synthèse | 0 | 0 | 0 | 0 | |
| Disponibilité | Synthèse | 1 | 0 | 1 | 1 | |
| Intégrité | Synthèse | 2 | 0 | 2 | 2 | |

### 4.2.3 Synthèse des fiches de besoins de sécurité

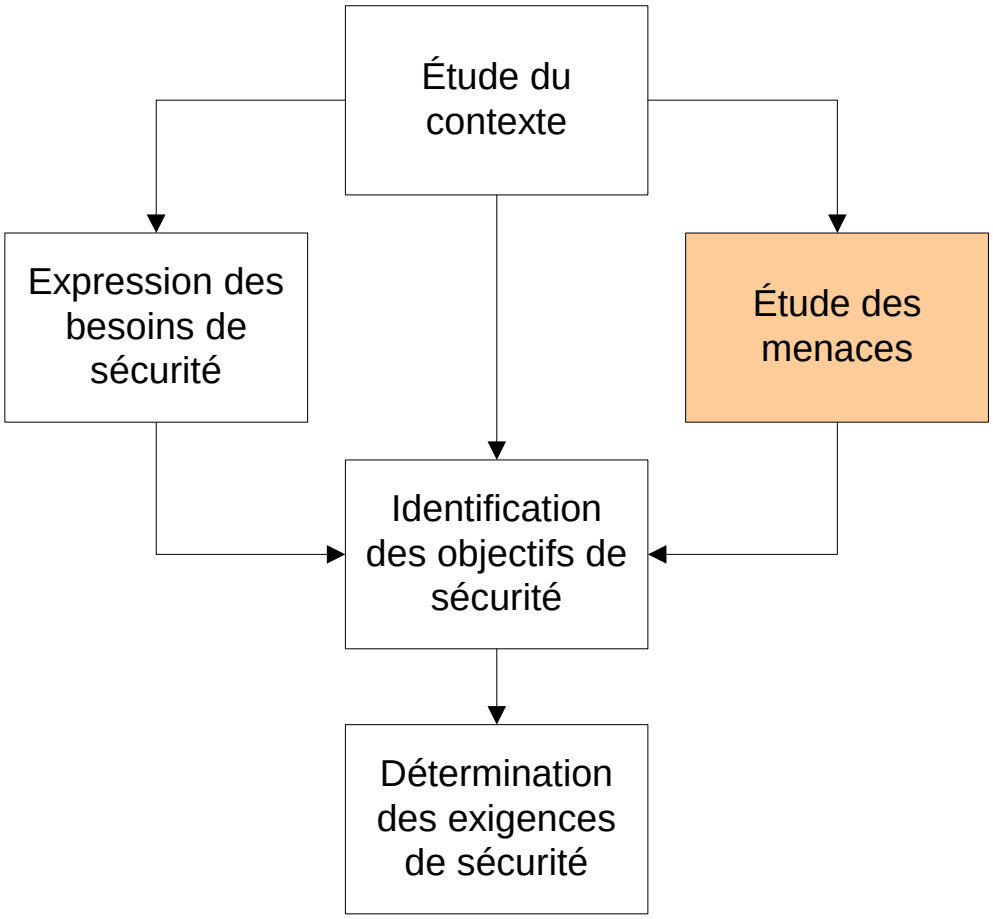
*Nous rassemblons les résultats de l'expression des besoins de sécurité dans des tableaux de synthèse, soit en reprenant chaque personne interrogée, soit en sélectionnant des personnes représentatives, soit encore en effectuant un calcul (maximum ou moyenne) par type d'utilisateur.*

*Nous synthétisons ensuite les valeurs par critère pour chaque élément essentiel et nous faisons valider les synthèses par le responsable utilisateur.*

| | | Commercial | Comptable | Ingénieur | Secrétaire | Technicien | Besoin de sécurité | Commentaires |
|---|---|---|---|---|---|---|---|---|
| I.CDC | Confidentialité | 1 | | | | | 1 | |
| | Disponibilité | 2 | | | | | 2 | |
| | Intégrité | 4 | | | | | 4 | Doit être juste |
| I.CONTRAT | Confidentialité | 1 | | | | | 1 | |
| | Disponibilité | 2 | | | | | 2 | |
| | Intégrité | 4 | | | | | 4 | Doit être juste |
| I.CONTX | Confidentialité | 1 | | 1 | | 1 | 1 | |
| | Disponibilité | 2 | | 2 | | 2 | 2 | |
| | Intégrité | 4 | | 4 | | 4 | 4 | Doit être juste |
| I.DEVIS | Confidentialité | 1 | | | | | 1 | |
| | Disponibilité | 2 | | | | | 2 | |
| | Intégrité | 4 | | | | | 4 | Doit être juste |
| I.DOSS | Confidentialité | | | 1 | | 1 | 1 | |
| | Disponibilité | | | 3 | | 3 | 3 | |
| | Intégrité | | | 4 | | 4 | 4 | Doit être juste |
| I.FACT | Confidentialité | | 1 | | | | 1 | |
| | Disponibilité | | 2 | | | | 2 | |
| | Intégrité | | 4 | | | | 4 | Doit être juste |
| I.PARA | Confidentialité | | | | | 2 | 2 | |
| | Disponibilité | | | | | 2 | 2 | |
| | Intégrité | | | | | 4 | 4 | Doit être juste |
| I.PLAN | Confidentialité | 0 | | 0 | | 0 | 0 | Public |
| | Disponibilité | 2 | | 2 | | 1 | 2 | |
| | Intégrité | 4 | | 4 | | 4 | 4 | Doit être juste |
| I.STRUC | Confidentialité | 0 | | 0 | | 0 | 0 | Public |
| | Disponibilité | 3 | | 2 | | 2 | 2 | |
| | Intégrité | 4 | | 4 | | 4 | 4 | Doit être juste |
| I.TECH | Confidentialité | 2 | | | | | 2 | |
| | Disponibilité | 3 | | | | | 3 | |
| | Intégrité | 4 | | | | | 4 | Doit être juste |
| I.VISU | Confidentialité | 0 | | 0 | | 0 | 0 | Public |
| | Disponibilité | 2 | | 2 | | 1 | 2 | |
| | Intégrité | 2 | | 0 | | 0 | 2 | |
| F.CONTX | Confidentialité | 0 | 0 | 0 | | | 0 | Public |

| | | Commercial | Comptable | Ingénieur | Secrétaire | Technicien | Besoin de sécurité | Commentaires |
|---|---|---|---|---|---|---|---|---|
| | Disponibilité | 1 | 2 | 1 | | | 2 | |
| | Intégrité | 4 | 4 | 4 | | | 4 | Exactitude requise |
| F.CPTA | Confidentialité | | 0 | | 0 | | 0 | Public |
| | Disponibilité | | 2 | | 1 | | 2 | |
| | Intégrité | | 4 | | 4 | | 4 | Exactitude requise |
| F.DEVIS | Confidentialité | 0 | | 0 | | 0 | 0 | Public |
| | Disponibilité | 2 | | 1 | | 2 | 2 | |
| | Intégrité | 4 | | 2 | | 2 | 4 | Exactitude requise |
| F.PLAN | Confidentialité | 0 | | 0 | | 0 | 0 | Public |
| | Disponibilité | 3 | | 2 | | 2 | 3 | |
| | Intégrité | 4 | | 4 | | 4 | 4 | Exactitude requise |
| F.PROJET | Confidentialité | 0 | | 0 | 0 | 0 | 0 | Public |
| | Disponibilité | 2 | | 2 | 1 | 1 | 2 | |
| | Intégrité | 2 | | 2 | 2 | 2 | 2 | |
| F.STRUC | Confidentialité | 0 | | 0 | | 0 | 0 | Public |
| | Disponibilité | 2 | | 2 | | 2 | 2 | |
| | Intégrité | 4 | | 4 | | 4 | 4 | Erreur inacceptable |
| F.VISU | Confidentialité | 0 | | 0 | | 0 | 0 | Public |
| | Disponibilité | 2 | | 2 | | 1 | 2 | |
| | Intégrité | 2 | | 0 | | 2 | 2 | |

# 5 Étape 3 : Étude des menaces




*Nous allons nous intéresser aux menaces pouvant affecter la cible de l'étude. Nous allons donc déterminer les méthodes d'attaques et les éléments menaçants qui pèsent sur la cible, puis les vulnérabilités associées exploitables. Il sera alors possible de décrire les différentes menaces auxquelles la cible peut être confrontée.*

## 5.1 Activité 3.1 : Étude des origines des menaces

*Il faut tout d'abord sélectionner les méthodes d'attaque pertinentes pour la cible et justifier le fait que certaines méthodes d'attaques ne sont pas retenues.*
*Pour les méthodes d'attaque retenues, il convient de déterminer les critères de sécurité qui peuvent être affectés (disponibilité, intégrité, confidentialité…) et qualifier les éléments qui peuvent en être à l'origine en termes de types (naturel, humain, environnemental) et de causes (accidentelle, délibérée). Nous pourrons aussi déterminer le potentiel d'attaque de chaque élément menaçant en fonction de sa caractérisation. En effet, si la cause est accidentelle, il convient d'évaluer l'exposition et les ressources disponibles ; si la cause est délibérée, il convient d'évaluer l'expertise, les ressources disponibles et la motivation. Il est ainsi possible de synthétiser cette évaluation par une valeur représentant le potentiel d'attaque. Ceci permettra de déterminer un niveau de résistance adéquat aux objectifs de sécurité.*

### 5.1.1 Méthodes d'attaque retenues

| 01- INCENDIE | |
|---|---|
| Atteintes | Intégrité<br>Disponibilité |
| Causes d'élément menaçant | Accidentelle<br>Délibérée |
| Potentiel d'attaque | Moyen (par exemple opportunités ou ressources limitées) |
| Types d'éléments menaçants | Environnemental<br>Humain<br>Naturel |
| Descriptions des éléments menaçants | Cause accidentelle<br>----------<br>Évènement extérieur ou un accident interne.<br><br>Exemples<br>----------<br>Foudre, feu de corbeille à papier, court-circuit.<br><br>Cause délibérée<br>----------<br>Terroristes, ancien employé cherchant à se venger ou vandale accédant aux biens pour provoquer la mise à feu directement ou indirectement (bombes incendiaires, altération des dispositifs de ventilation..) de matières inflammables ou explosives.<br><br>Exemples<br>----------<br>Personne accédant à un accès aux locaux pour y déposer un engin incendiaire. |

| 13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION | |
|---|---|
| Atteintes | Disponibilité |
| Causes d'élément menaçant | Accidentelle<br>Délibérée |
| Potentiel d'attaque | Faible (par exemple accidentel et aléatoire) |
| Types d'éléments menaçants | Environnemental |

| | |
|---|---|
| | Humain |
| Descriptions des éléments menaçants | Cause accidentelle<br>----------<br>Perturbation, arrêt ou mauvais dimensionnement des services de télécommunication (téléphone, accès Internet, réseau Internet).<br><br>Exemples<br>----------<br>Grèves, évènement extérieur exceptionnel provoquant la saturation des communications.<br><br>Cause délibérée<br>----------<br>Sabotage ou perturbation de l'installation Télécom par une personne accédant aux dispositifs de télécommunication (tête de ligne, PABX, Répartiteur, câbles extérieurs...).<br><br>Exemples<br>----------<br>Coupure volontaire des câbles Télécom, destruction d'un central Télécom extérieur, saturation volontaire de la bande passante Télécom. |

**19 - ÉCOUTE PASSIVE**

| | |
|---|---|
| Atteintes | Confidentialité |
| Causes d'élément menaçant | Délibérée |
| Potentiel d'attaque | Moyen (par exemple opportunités ou ressources limitées) |
| Types d'éléments menaçants | Humain |
| Descriptions des éléments menaçants | Cause délibérée<br>----------<br>Personne étant connectée aux équipements ou aux supports de communication ou placée dans le périmètre de couverture d'émission d'une communication. Elle utilise alors des moyens, qui peuvent être peu coûteux, pour écouter, sauvegarder et analyser les informations qui circulent (voix ou données).<br><br>Exemples<br>----------<br>L'interception peut avoir lieu sur des communications utilisant les technologies sans fil ou sur des signaux hertziens.<br>Dans le cas d'un support filaire, un équipement déjà connecté au réseau (par exemple poste de travail situé sur un réseau local), peut être utilisé par un employé soudoyé par la concurrence pour stocker et analyser les informations qui circulent (par exemple les informations échangées avec un serveur). De nombreux appareils du commerce facilitent les analyses et permettent d'interpréter en temps réel les trames quels que soient les protocoles de communication. |

**20 - VOL DE SUPPORTS OU DE DOCUMENTS**

| | |
|---|---|
| Atteintes | Confidentialité |
| Causes d'élément menaçant | Délibérée |
| Potentiel d'attaque | Moyen (par exemple opportunités ou ressources limitées) |
| Types d'éléments | Humain |

| | |
|---|---|
| menaçants | |
| Descriptions des éléments menaçants | Cause délibérée<br>----------<br>Personne interne ou externe à l'organisme accédant à des supports numériques ou des documents papiers dans le but de voler et d'exploiter les informations qui se trouvent sur ces supports.<br><br>Exemples<br>----------<br>Vol de disquettes, cd-rom, cartouches, bandes de sauvegarde.<br>Vol de dossiers, notes, plans, rapports.<br>Vol d'éditions laissées temporairement sur des imprimantes situées dans des locaux partagés.<br>Fouille des corbeilles, des poubelles entreposées sur la voie publique, de la part d'un employé désirant informer la concurrence en échange d'une rétribution. |

**21 - VOL DE MATÉRIELS**

| | |
|---|---|
| Atteintes | Confidentialité<br>Disponibilité |
| Causes d'élément menaçant | Délibérée |
| Potentiel d'attaque | Moyen (par exemple opportunités ou ressources limitées) |
| Types d'éléments menaçants | Environnemental<br>Humain |
| Descriptions des éléments menaçants | Cause délibérée<br>----------<br>Personne interne ou externe à l'organisme accédant au matériel, placé dans l'organisme ou transporté à l'extérieur, dans un but cupide ou stratégique.<br><br>Exemples<br>----------<br>Vol de micro-ordinateur portable de la part d'un intervenant externe, pour revendre le matériel<br>Vol d'un PDA pour exploiter son contenu. |

**23 - DIVULGATION**

| | |
|---|---|
| Atteintes | Confidentialité |
| Causes d'élément menaçant | Accidentelle<br>Délibérée |
| Potentiel d'attaque | Faible (par exemple accidentel et aléatoire) |
| Types d'éléments menaçants | Humain |
| Descriptions des éléments menaçants | Cause accidentelle<br>----------<br>Personne interne à l'organisme qui, par négligence, diffuse de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître ou à l'extérieur (les conséquences étant généralement plus importantes vis-à-vis de l'extérieur).<br><br>Exemples<br>---------- |

| | |
|---|---|
| | Erreur de destinataires lors d'envoi de message.<br>Réponse à des sollicitations sans vérification de l'origine (demande malveillante de mots de passe).<br>Non-connaissance des règles de diffusion de l'information, appliquées dans l'organisme.<br>Négligence commise dans la définition des règles de contrôle d'accès d'informations partagées.<br>Non-respect des règles élémentaires de discrétion (discussion ou lecture de document dans des lieux publics).<br><br>Cause délibérée<br>---<br>Personne diffusant consciemment de l'information au sein de l'organisme à d'autres personnes n'ayant pas le besoin d'en connaître ou à l'extérieur (les conséquences étant généralement plus importantes vis-à-vis de l'extérieur).<br><br>Exemples<br>---<br>Personne diffusant par messagerie des informations confidentielles par vengeance.<br>Personne divulguant de l'information considérant que la détention d'informations sensibles lui donne un certain pouvoir sur les autres.<br>Diffusion d'informations à un tiers sous pression d'un chantage.<br>Exploitation financière d'informations industrielles ou commerciales (espionnage industriel). |

## 26 - PIÉGEAGE DU LOGICIEL

| | |
|---|---|
| Atteintes | Intégrité<br>Confidentialité<br>Disponibilité |
| Causes d'élément menaçant | Accidentelle |
| Potentiel d'attaque | Moyen (par exemple opportunités ou ressources limitées) |
| Types d'éléments menaçants | Environnemental |
| Descriptions des éléments menaçants | Cause accidentelle<br>---<br>Action involontaire effectuée avec des moyens logiciels depuis l'intérieur ou l'extérieur de l'organisme conduisant à l'altération, la destruction de programmes ou de données, porter atteinte au bon fonctionnement de la ressource, voire exécuter des commandes au nom et à l'insu des usagers.<br><br>Exemples<br>---<br>Utilisateur connectant au réseau un micro-ordinateur portable infecté par un virus, introduit lors d'un échange avec un autre organisme.<br>Usager du système d'information recevant de l'extérieur de l'organisme un ver et le propageant à son insu à l'intérieur de l'organisme. |

## 42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL

| | |
|---|---|
| Atteintes | Disponibilité |
| Causes d'élément menaçant | Accidentelle |
| Potentiel d'attaque | Faible (par exemple accidentel et aléatoire) |
| Types d'éléments | Environnemental<br>Humain |

| | |
|---|---|
| menaçants | Humain |
| Descriptions des éléments menaçants | Cause accidentelle<br>----------<br>Absence de personnel qualifié ou habilité suite à un empêchement indépendant de la volonté des personnes.<br><br>Exemples<br>----------<br>Maladie, décès, grève de transport. |

### 5.1.2 Méthodes d'attaque non retenues

| | |
|---|---|
| **02- DÉGÂTS DES EAUX** | |
| Justification | Méthode d'attaque écartée par le comité de pilotage (traitée par ailleurs) |
| **03 - POLLUTION** | |
| Justification | Méthode d'attaque écartée par le comité de pilotage |
| **04 - SINISTRE MAJEUR** | |
| Justification | Méthode d'attaque écartée par le comité de pilotage |
| **05 - DESTRUCTION DE MATÉRIELS OU DE SUPPORTS** | |
| Justification | Méthode d'attaque écartée par le comité de pilotage |
| **06 - PHÉNOMÈNE CLIMATIQUE** | |
| Justification | Méthode d'attaque écartée par le comité de pilotage |
| **07 - PHÉNOMÈNE SISMIQUE** | |
| Justification | Méthode d'attaque jugée trop improbable |
| **08 - PHÉNOMÈNE VOLCANIQUE** | |
| Justification | Méthode d'attaque jugée trop improbable |
| **09 - PHÉNOMÈNE MÉTÉOROLOGIQUE** | |
| Justification | Méthode d'attaque écartée par le comité de pilotage |
| **10 - CRUE** | |
| Justification | Méthode d'attaque jugée trop improbable |
| **11 - DÉFAILLANCE DE LA CLIMATISATION** | |
| Justification | Méthode d'attaque écartée par le comité de pilotage (traitée par ailleurs) |
| **12 - PERTE D'ALIMENTATION ÉNERGÉTIQUE** | |
| Justification | Méthode d'attaque écartée par le comité de pilotage (traitée par ailleurs) |
| **14 - RAYONNEMENTS ÉLECTROMAGNÉTIQUES** | |
| Justification | Méthode d'attaque jugée trop improbable |
| **15 - RAYONNEMENTS THERMIQUES** | |
| Justification | Méthode d'attaque jugée trop improbable |
| **16 - IMPULSIONS ÉLECTROMAGNÉTIQUES** | |
| Justification | Méthode d'attaque jugée trop improbable |
| **17 - INTERCEPTION DE SIGNAUX PARASITES COMPROMETTANTS** | |
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 18 - ESPIONNAGE A DISTANCE | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 22 - RÉCUPÉRATION DE SUPPORTS RECYCLÉS OU MIS AU REBUS | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 24 - INFORMATIONS SANS GARANTIE DE L'ORIGINE | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 25 - PIÉGEAGE DU MATÉRIEL | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 27 - GÉOLOCALISATION | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 28 - PANNE MATÉRIELLE | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage (gérée par la maintenance) |

| 29 - DYSFONCTIONNEMENT DU MATÉRIEL | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage (gérée par la maintenance) |

| 30 - SATURATION DU SYSTÈME INFORMATIQUE | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 31 - DYSFONCTIONNEMENT LOGICIEL | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 32 - ATTEINTE À LA MAINTENABILITÉ DU SYSTÈME D'INFORMATION | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 33 - UTILISATION ILLICITE DES MATÉRIELS | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 34 - COPIE FRAUDULEUSE DE LOGICIELS | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 35 - UTILISATION DE LOGICIELS CONTREFAITS OU COPIÉS | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage (moyens budgétaires affectés aux achats des licences des logiciels nécessaires) |

| 36 - ALTÉRATION DES DONNÉES | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 37 - TRAITEMENT ILLICITE DES DONNÉES | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 38 - ERREUR D'UTILISATION | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 39 - ABUS DE DROIT | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 40 - USURPATION DE DROIT | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

| 41 - RENIEMENT D'ACTIONS | |
|---|---|
| Justification | Méthode d'attaque écartée par le comité de pilotage |

## 5.2 Activité 3.2 : Étude des vulnérabilités

*Pour chaque méthode d'attaque retenue, nous déterminons les vulnérabilités pertinentes qui peuvent être exploitées par les éléments menaçants par type d'entité. Nous attribuons alors une valeur à ces vulnérabilité (potentialité, fréquence ou faisabilité selon le contexte…) par type d'entité touché.*

*L'échelle des valeurs de vulnérabilités est la suivante :*

| | |
|---|---|
| *0* | *totalement improbable ou infaisable* |
| *1* | *faiblement probable ou nécessite des moyens très importants et/ou des connaissances très élevées dans le domaine considéré* |
| *2* | *moyennement probable ou nécessite un certain niveau d'expertise et/ou du matériel spécifique* |
| *3* | *fortement probable ou réalisable avec des moyens standards et/ou avec des connaissances de base* |
| *4* | *certain ou réalisable par tout public* |

Voici les vulnérabilités pertinentes pour le cabinet d'études et leur niveau selon les entités concernées :

01- INCENDIE

| | E.ARC+ | E.BUR | E.CAO | E.COMM | E.CPTA | E.CRM | E.DIR | E.EDF | E.EXP | E.FSI | E.ING | E.MAGN | E.MESS | E.OFFI | E.ORGA | E.PAO | E.PAP | E.PGMK | E.PLAN | E.PORTA | E.SECR | E.SERV | E.SIFRA | E.SITE | E.SPOT | E.TECH | E.TEL | E.WNT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Absence d'affichage des informations à jour pour l'appel des services d'urgence | | | | | | | | | | | | | | | 2 | | | | | | | | | | | | | |
| Absence d'organisation de lutte contre l'incendie (description des rôles, responsabilités) | | | | | | | | | | | | | | | 3 | | | | | | | | | | | | | |
| Absence de cloisonnement anti-feu | | | | | | | | | | | | | | | | | | | | | | | | 4 | | | | |
| Absence de contrôle d'accès au site ou aux locaux | | | | | | | | | | | | | | | | | | | | | | | | 4 | | | | |
| Absence de couverture d'assurance en cas de sinistre grave | | | | | | | | | | | | | | | 0 | | | | | | | | | | | | | |
| Absence de gestion des procès verbaux de contrôle des équipements de secours | | | | | | | | | | | | | | | 3 | | | | | | | | | | | | | |
| Absence de matériels de remplacement | | 1 | 3 | | | 3 | | | | | | | | | | 2 | | | 1 | 3 | | 4 | | | | | | |
| Absence de prise en compte dans la phase d'installation des risques d'incendie spécifiques aux équipements hébergés | | | | | | | | 2 | | 2 | | | | | | | | | | | | | | | | 2 | | |
| Absence de sauvegarde des données contenues sur les supports | | | | | | | | | | | | 2 | | | | | | | | | | | | | | | | |
| Absence de sensibilisation à la protection des équipements de sécurité | | | | | | | 3 | | | | | | | | | | | | | | | | | | | | | |
| Absence de suivi des contrats de maintenance des équipements de protection incendie | | | | | | | | | | | | | | | 3 | | | | | | | | | | | | | |
| Absence de test des procédures de réaction et | 4 | | | 4 | 4 | | 3 | | 2 | | 2 | | | | | | | | | | 4 | | | | | 2 | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Absence ou mauvais dimensionnement ou inadéquation du dispositif d'extinction automatique d'incendie | | | | | | | | 2 | | 2 | | | | | | | | | | | | | | | | | 2 | |
| Exemplaire unique des contrats de licence | 4 | | | | | | | | | | | | 4 | 4 | | | | 4 | | | | | 4 | | 4 | | | 4 |
| Matériel utilisant des matériaux inflammables (ex. : imprimantes de masse provoquant des poussières) | | 2 | 2 | | | 2 | | | | | | | | | | 2 | | | 2 | 2 | | 2 | | | | | | |
| Méconnaissance des mesures de sécurité | | | | 3 | 2 | | 2 | | 1 | | 1 | | | | | | | | | | 3 | | | | | 2 | | |
| Présence d'ouverture sur la voie publique (fenêtre) | | | | | | | | 0 | | 0 | | | | | | | | | | | | | | 4 | | | 0 | |
| Supports originaux | | | | | | | | | | | | | | | | | 2 | | | | | | | | | | | |
| Vieillissement des locaux | | | | | | | | | | | | | | | | | | | | | | | | 1 | | | | |

13 – PERTE DES MOYENS DE TÉLÉCOMMUNICATION

| | E.BUR | E.CAO | E.COMM | E.CPTA | E.CRM | E.DIR | E.EDF | E.EXP | E.FSI | E.ING | E.ORGA | E.PAO | E.PLAN | E.PORTA | E.SECR | E.SERV | E.TECH | E.TEL |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Absence de consignes (alerte, prévention, réaction…) | | | | | | | | | | | 3 | | | | | | | |
| Absence de maintenance des équipements de terminaison et de distribution | | | | | | | | | 3 | | | | | | | | | 4 |
| Accès physique non protégé aux locaux hébergeant les équipements d'alimentation et de distribution électriques ou moyens de télécommunication | | | | | | | 2 | | 2 | | | | | | | | | 2 |
| Dysfonctionnement déjà constaté dans la fourniture du service de télécommunication | | | | | | | | | 1 | | | | | | | | | 1 |
| Défauts d'exploitation du réseau téléphonique interne | | | | | | | | | 1 | | | | | | | | | 1 |
| Matériel maintenu à distance par des moyens de télécommunication | 0 | 0 | | | 0 | | | | | | | 0 | 0 | 0 | | 0 | | |
| Méconnaissance des mesures de sécurité | | | 3 | 3 | | 2 | | 2 | | 2 | | | | | 3 | | 2 | |

19 - ÉCOUTE PASSIVE

| | E.ADSL | E.ARC+ | E.BUR | E.CAO | E.COMM | E.CPTA | E.CRM | E.DIR | E.ETH | E.EXP | E.FSI | E.ING | E.MESS | E.OFFI | E.ORGA | E.PAO | E.PGMK | E.PLAN | E.PORTA | E.SECR | E.SERV | E.SIFRA | E.SITE | E.SPOT | E.TECH | E.TEL | E.WNT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Absence d'identification des biens sensibles | | | | | | | | | | | | | | | 3 | | | | | | | | | | | | |
| Absence de contrôle d'accès au site ou aux locaux ou possibilité de pénétrer par des accès indirects | | | | | | | | | | | | | | | | | | | | | | | 4 | | | | |
| Absence de contrôle de l'application de la politique de sécurité | | | | | | | | | | | | | | | 4 | | | | | | | | | | | | |
| Absence de dispositif de contrôle d'accès en cas d'inactivité | | 1 | | | | | | | | | | | 1 | 1 | | | 1 | | | | | 1 | | 1 | | | 2 |
| Absence de protection contre l'usage de privilèges avancés | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| Absence de protection des accès aux équipements terminaux de communication | | | | | | | | | | | 3 | | | | | | | | | | | | | | | 3 | |
| Absence de protection des journaux récoltant la trace des activités | | 2 | | | | | | | | | | | 2 | 0 | | | 2 | | | | | 2 | | 2 | | | |
| Absence de soutien de la direction à l'application de la politique de sécurité | | | | | 3 | 2 | | | | 2 | | 2 | | | | | | | | 3 | | | | | 2 | | |
| Accès logique au matériel permettant la pose d'un logiciel d'écoute | | | 4 | 3 | | | 3 | | | | | | | | | 3 | | 3 | 2 | | 3 | | | | | | |
| Faible sensibilisation à la protection en confidentialité des échanges d'information | | | | | 2 | 2 | | 2 | | 2 | | 2 | | | | | | | | 2 | | | | | 2 | | |
| La politique de sécurité n'est pas appliquée | | | | | | | | | | | | | | | 4 | | | | | | | | | | | | |
| Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées | | | | | | | | | | | | | | | 3 | | | | | | | | | | | | |
| Manque de formation aux mesures et outils de protection des échanges externe et interne | | | | | 3 | 3 | | 3 | | 1 | | 2 | | | | | | | | 3 | | | | | 2 | | |
| Matériel disposant d'interface de communication | | | 0 | 0 | | | 0 | | | | | | | | | 0 | | 0 | 2 | | 0 | | | | | | |

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| écoutable (infra rouge, 802.11, Bluetooth...) | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Médium et supports disposant des caractéristiques permettant l'écoute passive (ex:Ethernet, systèmes de communication sans fil) | 2 | | | | | | | | 2 | | | | | | | | | | | | | | | | | | | |
| Obtention d'un avantage à la captation d'information | | | | | 0 | 0 | | 0 | | 0 | | 0 | | | | | | | | 0 | | | | | 0 | | | |
| Pas ou peu de changement de mot de passe d'accès au système ou à l'application | | 3 | | | | | | | | | | | 3 | | | | 3 | | | | | 3 | | 3 | | | 2 |
| Possibilité d'ajout d'un logiciel d'écoute de type cheval de Troie | | 0 | | | | | | | | | | | 3 | 1 | | | 0 | | | | | 0 | | 0 | | | 2 |
| Support ou équipement de communication physiquement accessible permettant la pose d'un matériel d'écoute | 4 | | | | | | | | 4 | | | | | | | | | | | | | | | | | | | |

20 – VOL DE SUPPORTS OU DE DOCUMENTS

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Absence de protection d'accès aux équipements de sauvegarde | | | | | | | | 3 | | | | | | | | | | | | | | | | | | | | |
| Absence de protection du stockage des supports | | | | | | | | | | 2 | | | 3 | | | | | | | | | | | | | | | |
| Absence de sauvegarde des données contenues sur les supports | | | | | | | | | | 3 | | | | | | | | | | | | | | | | | | |

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Absence de sensibilisation à la protection des documents à caractère confidentiel provoquant un manque de vigilance | | | 3 | 2 | | 2 | 2 | | 2 | | | | | | | 3 | | | 2 |
| Absence de soutien de la direction à l'application de la politique de sécurité | | | | | | 3 | | | | | | | | | | | | | |
| Disque dur facilement démontable | 2 | 2 | | | 2 | | | | | | | 2 | | 2 | 1 | | 2 | | |
| La politique de sécurité n'est pas appliquée | | | | | | | | | | | 4 | | | | | | | | |
| Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous | | | | | | | | | | | 3 | | | | | | | | |
| Les supports sont accessibles par tous | | | | | | | | | | 2 | | | 3 | | | | | | |
| Matériels attractifs (valeurs marchande, technologique, stratégique) | 1 | 3 | | | 2 | | | | | | | 3 | | 2 | 4 | | 3 | | |
| Non-respect des règles associées à la classification des informations | | | 4 | 3 | | 3 | 3 | | 3 | | | | | | | 3 | | | 3 |
| Présence d'imprimante dans les lieux de passage | | | | | | | | 4 | | | | | | | | | | | |
| Supports aisément transportables (ex: disque dur extractible, cartouche de sauvegarde) | | | | | | | | | | 4 | | | | | | | | | |
| Supports originaux | | | | | | | | | | | | | 2 | | | | | | |
| Transmission des supports par des services postaux (fournisseurs externes, courrier interne,…) | | | | | | | | | | 0 | | | 3 | | | | | | |

21 - VOL DE MATÉRIELS

| | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Absence de règles de contrôle des entrées/sorties des matériels dans l'organisme | | | | | | | | | | 3 | | | | | | | | | | | | | | | | | | |
| Absence de soutien de la direction à l'application de la politique de sécurité | | | 3 | 2 | | | 1 | | 2 | | | | | 3 | | | 2 | | | | | | | | | | | |
| Faible sensibilisation à la protection des matériels en dehors de l'organisme | | | 3 | 2 | | 3 | 2 | | 2 | | | | | 3 | | | 3 | | | | | | | | | | | |
| Matériel facilement démontable | 2 | 2 | | | 2 | | | | | | 2 | 2 | | | 2 | | | | | | | | | | | | | |
| Matériels attractifs (valeurs marchande, technologique, stratégique) | | | | | | | | 3 | | | | | 4 | | | | | | | | | | | | | | | |
| Non-respect des règles de protection physique applicables aux équipements transportables | | | 2 | 2 | | 2 | 2 | | 1 | | | | | 2 | | | 1 | | | | | | | | | | | |

23 – DIVULGATION

| | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| La politique de sécurité n'est pas appliquée | | | | | | | | | | | | | | | | 3 | | | | | | | | | | | | | |
| Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous | | | | | | | | | | | | | | | | 3 | | | | | | | | | | | | | |
| Non-respect des règles de classification de l'information | | | | | 2 | 2 | | 2 | | 2 | | 2 | | | | | | | | | 2 | | | | | 2 | | | |
| Non-respect du devoir de réserve | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Obtention d'un avantage à la divulgation d'information | | | | | 0 | 0 | | 0 | | 0 | | 0 | | | | | | | | | 0 | | | | | 0 | | | |
| Procédures de gestion et d'application des habilitations trop lourde à exploiter | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Présence d'un réseau de communication avec l'extérieur permettant l'échange d'information | 4 | | | | | | | | 1 | | | | | | | | | | | | | | | | | | | | |
| Présence de répertoire partagé pour stocker de l'information | | | 4 | 4 | | | 4 | | | | | | | | | | 4 | | | 4 | | 4 | | | | | | |
| Supports capables d'effectuer des échanges d'information à caractère sensible | | | | | | | | | | | | | 4 | | | | | 4 | | | | | | | | | | | |

26 - PIÉGEAGE DU LOGICIEL

| | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E | E |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|

| | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| logiciels | | | | | | | | | | | | | | | | | | | | | | | | | | |
| Absence de moyens permettant le contrôle d'innocuité des supports lors de leurs entrées dans l'organisme | | | | | | | | | | | 4 | | | | | | | | | | | | | | | |
| Absence de politique de conservation et d'analyse des traces des activités | | | | | | | | | | | | | | 3 | | | | | | | | | | | | |
| Absence de politique de protection des postes de travail | | | | | | | | | | | | | | 4 | | | | | | | | | | | | |
| Absence de politique globale de lutte contre le code malveillant | | | | | | | | | | | | | | 4 | | | | | | | | | | | | |
| Absence de protection contre l'usage de privilèges avancés | 4 | | | | | | | | | | | 4 | 4 | | | 4 | | | | | 4 | | 4 | | | |
| Insuffisance de la complexité des mots de passe de connexion | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| La couche SNMP est activée | | | | | | | | | | | | | | | | | | | | | | | | | | 0 |
| La liaison de télémaintenance est activée en permanence | 0 | | | | | | | | | | | 0 | 0 | | | 0 | | | | | 0 | | 0 | | | 0 |
| Le matériel est amorçable par tous à partir d'un périphérique (ex. : disquette, cédérom) | | 4 | 4 | | | 4 | | | | | | | | | 4 | | 4 | 4 | | 4 | | | | | | |
| Manque de sensibilisation à la menace des codes malveillants | | | | 3 | 2 | | 3 | 1 | | 2 | | | | | | | | | 4 | | | | | 3 | | |
| Méconnaissance des procédures d'intervention en cas de détection d'anomalie | | | | | | | | 3 | | | | | | | | | | | | | | | | | | |
| Méconnaissance des réactions réflexes en cas de détection d'anomalie | | | | 3 | 2 | | 3 | | | 2 | | | | | | | | | 4 | | | | | 4 | | |
| Non-respect des règles de mises à jour des logiciels anti-virus | | | | 3 | 1 | | 2 | 0 | | 1 | | | | | | | | | 2 | | | | | 2 | | |
| Possibilité d'effacer, de modifier ou d'installer des nouveaux programmes | | | | | | | | | | | | | | | | | | | | | | | | | | 3 |
| Possibilité d'installer des correctifs, mises à jours, patches, hotfixes... | | | | | | | | | | | | | | | | | | | | | | | | | | 3 |
| Utilisation d'un système d'exploitation standard pour lequel des attaques logiques ont déjà été réalisées | | | | | | | | | | | | | | | | | | | | | | | | | | 4 |

42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL

| | E.ADSL | E.BUR | E.CAO | E.COMM | E.CPTA | E.CRM | E.DIR | E.ETH | E.EXP | E.ING | E.MAGN | E.ORGA | E.PAO | E.PAP | E.PLAN | E.PORTA | E.SECR | E.SERV | E.SITE | E.TECH |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Absence d'équipe de protection du personnel | | | | | | | | | | | | 4 | | | | | | | | |
| Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles | | | | | | | | | | | | 4 | | | | | | | | |
| Absence de processus de gestion de la continuité des activités professionnelles de l'organisme | | | | | | | | | | | | 4 | | | | | | | | |
| Absence de procédure d'archivage | | | | | | | | | | | 4 | | | 2 | | | | | | |
| Absence de procédures de transfert de connaissances | | | | 2 | 3 | | | | | 2 | | 3 | | | | | 3 | | | 2 |
| Indisponibilité causée par l'absentéisme | | | | 1 | 1 | | | | 1 | 1 | | | | | | | 1 | | | 0 |
| Indisponibilité causée par la maladie | | | | 1 | 1 | | | | 1 | 1 | | | | | | | 1 | | | 1 |
| Indisponibilité provoquée (agression physique, prise d'otage...) | | | | 0 | 0 | | | | 0 | 0 | | | | | | | 0 | | | 0 |
| Indisponibilité provoquée par un enjeu concurrentiel | | | | | | | 1 | | | | | | | | | | | | | |
| Personnels habitant loin des locaux | | | | | | | | | | | | | | | | | | | 2 | |
| Personnels spécialisés hébergés dans des locaux distants | | | | | | | | | | | | | | | | | | | 0 | |
| Possibilité de nuisances pour le personnel utilisateur (transmission par voie hertzienne, ondes...) | 0 | | | | | | | 0 | | | | | | | | | | | | |
| Possibilité que certains matériels provoquent des nuisances pour le personnel utilisateur (travail devant écran, ondes...) | | 2 | 2 | | | 2 | | | | | | | 2 | | 2 | 2 | | 1 | | |
| Présence d'une épidémie virale locale | | | | | | | | | | | | 2 | | | | | | | | |

## 5.3 Activité 3.3 : Formalisation des menaces

*Nous pouvons maintenant créer un tableau des menaces en associant les méthodes d'attaque des éléments menaçants et les vulnérabilités retenues. Nous y rappelons les critères de sécurité touchés (Disponibilité, Intégrité, Confidentialité…) et la valeur des vulnérabilités.*

*Si une méthode d'attaque exploite plusieurs vulnérabilités pour se réaliser, alors il convient de déterminer l'opportunité de la menace en fonction des valeurs des vulnérabilités exploitées.*

*Si une méthode d'attaque n'exploite qu'une seule vulnérabilité pour se réaliser, alors l'opportunité de la menace est égale à la valeur de cette vulnérabilité.*

La liste suivante présente les 39 menaces identifiées :

| **M.INCENDIE-PHY** | |
|---|---|
| Méthode d'attaque | 01- INCENDIE |
| Description | Aggravation des conséquences d'un incendie accidentel ou délibéré, à cause de l'absence de prise en compte des risques d'incendie dans la phase d'installation du central téléphonique et du réseau électrique. |
| Opportunité | 2 |

| **M.INCENDIE-SITE** | |
|---|---|
| Méthode d'attaque | 01- INCENDIE |
| Description | Un terroriste ou un concurrent profite de la présence d'ouverture sur la voie publique ainsi que les absences de cloisonnement anti-feu et de contrôle d'accès au sein du site pour déclencher un incendie. |
| Opportunité | 4 |

| **M.INCENDIE-SUPPORT** | |
|---|---|
| Méthode d'attaque | 01- INCENDIE |
| Description | Un incendie causé de façon accidentelle (la foudre, un court-circuit) ou intentionnelle (un terroriste ou un concurrent) est aggravé par l'absence de sauvegarde des données contenues sur le matériel transportable. |
| Opportunité | 2 |

| **M.INCENDIE-PER** | |
|---|---|
| Méthode d'attaque | 01- INCENDIE |
| Description | Un incendie dû à un évènement intentionnel (un terroriste, un concurrent) ou accidentel (la foudre, un court-circuit) est aggravé compte tenu de l'absence de test des procédures de réaction et d'information, ainsi que par la méconnaissance des mesures de sécurité de la part du personnel. |
| Opportunité | 4 |

| **M.INCENDIE-ORGA** | |
|---|---|
| Méthode d'attaque | 01- INCENDIE |
| Description | Un incendie déclenché de façon volontaire (un terroriste ou un concurrent) ou par accident (foudre, court-circuit) est aggravé par l'absence :<br>- de procédures de sauvegarde des donnés contenues sur les supports,<br>- d'organisation de lutte contre l'incendie,<br>- d'affichage des informations à jour pour l'appel des services d'urgence. |
| Opportunité | 3 |

| M.INCENDIE-LOG | |
|---|---|
| Méthode d'attaque | 01- INCENDIE |
| Description | Un incendie ayant une origine accidentelle (un court circuit ou la foudre) ou volontaire (un terroriste ou un concurrent malveillant), est aggravé du fait de l'unicité des exemplaires des contrats de licence des logiciels. |
| Opportunité | 4 |

| M.ICENDIE-MAT-FIXE | |
|---|---|
| Méthode d'attaque | 01- INCENDIE |
| Description | Un incendie accidentel (dû à la foudre ou à un court-circuit sur un produit inflammable) est aggravé par l'absence de matériels fixes de remplacement et du stockage de matériaux inflammables.<br><br>Un concurrent utilise des matériaux inflammables présents au sein de l'entreprise pour déclencher un incendie. |
| Opportunité | 3 |

| M.TELECOM-ORGA | |
|---|---|
| Méthode d'attaque | 13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION |
| Description | L'absence de maintenance des terminaux téléphoniques et Internet de la part de l'organisation aggrave la perte des moyens de télécommunication. |
| Opportunité | 3 |

| M.TELECOM-PER | |
|---|---|
| Méthode d'attaque | 13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION |
| Description | Un attaquant accédant aux dispositifs de télécommunication profite de la méconnaissance du personnel concernant les mesures de sécurité pour entraîner une perte des moyens de télécommunication. |
| Opportunité | 3 |

| M.TELECOM-PHY | |
|---|---|
| Méthode d'attaque | 13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION |
| Description | La perturbation, l'arrêt ou le mauvais dimensionnement des services de télécommunication entraîne une perte des moyens de télécommunications de manière accidentelle à cause :<br>- d'un dysfonctionnement des réseaux externes,<br>- d'un défaut d'exploitation du réseau téléphonique interne,<br>- de l'absence de la maintenance des équipements de télécommunication,<br>- de l'absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service d'accès à Internet ou téléphonique.<br><br>Un concurrent exploite le fait que l'accès physique des locaux hébergeant les moyens de télécommunication ne soit pas protégé pour attaquer les moyens de télécommunication. |
| Opportunité | 4 |

| M.ECOUTE-SITE | |
|---|---|
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Un concurrent, un intervenant extérieur ou une personne interne malveillante profite de l'absence de contrôle d'accès au site pour entrer dans les locaux afin d'exercer une écoute passive. |
| Opportunité | 4 |

| M.ECOUTE-RES | |
|---|---|
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Un concurrent, un intervenant extérieur ou une personne malveillante, utilise un médium (Téléphone, ADSL, câble Ethernet) permettant la pose de matériel d'écoute pour exercer une écoute passive. |
| Opportunité | 2 |

| M.ECOUTE-PHY | |
|---|---|
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Un intervenant extérieur, un concurrent ou une personne interne malveillante exerce une écoute passive grâce à l'absence de protection d'accès au modem ADSL et au central téléphonique. |
| Opportunité | 3 |

| M.ECOUTE-PER | |
|---|---|
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Une personne malveillante directement connectée au réseau exploite la faible sensibilisation à la protection en confidentialité des échanges d'information, l'absence de soutien de la direction à l'application de la politique de sécurité ou le manque de formation du personnel aux mesures et outils de protection des échanges externe et interne, pour exercer une écoute passive. |
| Opportunité | 3 |

| M.ECOUTE-ORGA | |
|---|---|
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Un attaquant connecté au réseau exerce une écoute passive en profitant :<br>- de l'absence d'identification des biens sensibles,<br>- de l'absence de contrôle de l'application de la politique de sécurité,<br>- de la politique de sécurité n'est pas appliquée,<br>- du fait que les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées. |
| Opportunité | 4 |

| M.ECOUTE-LOG | |
|---|---|
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Un attaquant utilisant les équipements ou supports de communication exploite les caractéristiques logiciel suivantes pour faire de l'écoute passive :<br>- absence de dispositif de contrôle accès en cas d'inactivité,<br>- absence de protection des journaux récoltant la trace des activités,<br>- absence de protection contre l'usage de privilèges avancés,<br>- pas de changement de mot de passe d'accès,<br>- possibilité d'ajout d'un logiciel d'écoute de type cheval de Troie. |
| Opportunité | 3 |

| M.VOL-DOC-PER | |
|---|---|
| Méthode d'attaque | 20 - VOL DE SUPPORTS OU DE DOCUMENTS |
| Description | Une personne interne à l'organisme, ou un intervenant externe vole un document ou un support en profitant de l'absence de sensibilisation à la protection des documents à caractère confidentiel ou du non respect des règles associées à la classification des informations de la part du personnel. |
| Opportunité | 3 |

| M.VOL-DOC-SITE | |
|---|---|
| Méthode d'attaque | 20 - VOL DE SUPPORTS OU DE DOCUMENTS |
| Description | Une personne externe s'introduit dans l'organisme pour voler des supports ou des documents, profitant de l'absence de contrôle d'accès au site. |
| Opportunité | 4 |

| M.VOL-DOC-SUPPORT | |
|---|---|
| Méthode d'attaque | 20 - VOL DE SUPPORTS OU DE DOCUMENTS |
| Description | Une personne malveillante effectue un vol de documents exploitant le fait que les supports soient accessibles par tous et aisément transportables.<br><br>Une personne interne ou externe à l'organisme effectue un vol de documents, profitant de l'absence d'inventaire ou de protection des supports.<br><br>Un vol de documents ou de support par une personne interne ou externe à l'organisme est aggravé par l'utilisation de supports originaux non sauvegardés. |
| Opportunité | 4 |

| M.VOL-DOC-ORGA | |
|---|---|
| Méthode d'attaque | 20 - VOL DE SUPPORTS OU DE DOCUMENTS |
| Description | Une personne interne à l'organisme ou extérieure effectue un vol de supports ou de documents en exploitant l'une des vulnérabilités de l'organisation suivante :<br>- absence d'identification des biens sensibles,<br>- absence d'organisation de gestion des incidents de sécurité,<br>- absence de contrôle de l'application de la politique de sécurité,<br>- absence de contrôle des biens sensibles,<br>- la politique de sécurité n'est pas appliquée,<br>- les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous. |
| Opportunité | 4 |

| M.VOL-DOC-MAT | |
|---|---|
| Méthode d'attaque | 20 - VOL DE SUPPORTS OU DE DOCUMENTS |
| Description | Une personne malveillante, un concurrent, ou une personne interne à l'organisme profite de l'absence d'inventaire du matériel, des disques durs facilement démontables ou de la présence de matériels attractifs, pour voler un support ou un document. |
| Opportunité | 1 |

| M.VOL-MAT-ORGA | |
|---|---|
| Méthode d'attaque | 21 - VOL DE MATÉRIELS |
| Description | Un vol de matériels par une personne externe ou interne à l'organisme est aggravé par l'absence d'identification des biens sensibles ou de gestion des incidents de sécurité lié au vol.<br><br>Une personne interne ou externe à l'organisme exploite l'absence de contrôle de l'application de la politique de sécurité pour effectuer un vol de matériel.<br><br>Un personne externe utilise les entrées/sorties des matériels dans l'organisation pour effectuer un vol de matériel. |
| Opportunité | 4 |

| M.VOL-MAT-PER | |
|---|---|
| Méthode d'attaque | 21 - VOL DE MATÉRIELS |
| Description | Une personne externe à l'organisme vole du matériel en exploitant l'absence de soutien de la direction à l'application de la politique de sécurité, la faible sensibilisation à la protection des matériels en dehors de l'organisme ou le non-respect des règles de protection des équipements transportables de la part du personnel. |
| Opportunité | 3 |

| M.VOL-MAT-SITE | |
|---|---|
| Méthode d'attaque | 21 - VOL DE MATÉRIELS |
| Description | Une personne externe, profitant de l'absence de contrôle d'accès au site, s'infiltre au sein de l'organisme et vole des matériels. |
| Opportunité | 4 |

| M.VOL-MAT-MAT | |
|---|---|
| Méthode d'attaque | 21 - VOL DE MATÉRIELS |
| Description | Une personne interne ou externe à l'organisme vole des matériels du fait de l'utilisation de matériels attractifs, démontables ou de l'absence d'inventaire.<br><br>Le vol de matériels par une personne interne ou externe à l'organisme est aggravé par l'absence de matériel de remplacement. |
| Opportunité | 3 |

| M.DIV-SUP | |
|---|---|
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne interne divulgue de façon délibérée ou non des informations, grâce à l'utilisation de supports capables d'effectuer des échanges d'information à caractère sensible (papier, clé USB, disquette...). |
| Opportunité | 4 |

| M.DIV-PHY | |
|---|---|
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne interne diffuse de façon délibérée ou non des informations du fait de l'absence de contrôle des échanges avec l'extérieur. |
| Opportunité | 4 |

| M.DIV-PER | |
|---|---|
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne interne divulgue de façon délibérée ou non des renseignements du fait du non-respect des règles de classification de l'information ou de l'absence de sensibilisation à la protection de l'information à caractère sensible et de soutien de la direction à l'application de la politique de sécurité vis-à-vis du personnel. |
| Opportunité | 3 |

| M.DIV-ORGA | |
|---|---|
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne interne diffuse des informations de façon involontaire ou délibérée, du fait de la présence de vulnérabilités dans l'organisation :<br>- absence d'identification des biens sensibles,<br>- absence d'organisation responsable de la définition, de la mise en oeuvre et du contrôle des privilèges d'accès à l'information,<br>- absence de contrôle des biens sensibles,<br>- absence de politique de protection de l'information,<br>- la politique de sécurité n'est pas appliquée,<br>- les responsables sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous. |
| Opportunité | 4 |

| M.DIV-MAT | |
|---|---|
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne interne à l'organisme, diffuse par négligence de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître ou à l'extérieur du fait de l'absence de vérification des accès partagés accordés aux fonctions de gestion des droits d'accès trop compliquées à utiliser et pouvant être source d'erreur ou de la présence de répertoires partagés pour stocker de l'information. |
| Opportunité | 3 |

| M.DIV-LOG | |
|---|---|
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne interne à l'organisme qui, par négligence, du fait de l'absence de vérification des accès partagés accordés au niveau logiciel, diffuse de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître. |
| Opportunité | 3 |

| M.PIEGE-SUP | |
|---|---|
| Méthode d'attaque | 26 - PIÉGEAGE DU LOGICIEL |
| Description | Un utilisateur piège un logiciel du fait de l'absence de moyens permettant le contrôle d'innocuité des supports magnétiques (clé USB, disquette) lors de leurs entrées dans l'organisme. |
| Opportunité | 4 |

| M.PIEGE-LOG | |
|---|---|
| Méthode d'attaque | 26 - PIÉGEAGE DU LOGICIEL |
| Description | Une personne introduit de façon involontaire (une personne interne exécutant à son insu un virus) un logiciel ou des commandes de manière à modifier le comportement d'un logiciel grâce à l'absence de protection contre l'usage de privilèges avancés ou de mise en oeuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels. |
| Opportunité | 4 |

| M.PIEGE-MAT | |
|---|---|
| Méthode d'attaque | 26 - PIÉGEAGE DU LOGICIEL |
| Description | Un utilisateur légitime du système d'information amorce involontairement un matériel à partir d'un périphérique. |
| Opportunité | 4 |

| M.PIEGE-PER | |
|---|---|
| Méthode d'attaque | 26 - PIÉGEAGE DU LOGICIEL |
| Description | Un utilisateur piège involontairement un logiciel du fait :<br>- du manque de sensibilisation à la menace des codes malveillant,<br>- de la méconnaissance des procédures d'intervention et de réactions réflexes en cas de détection d'anomalie,<br>- du non-respect des règles de mises à jour des logiciels anti-virus, vis-à-vis du personnel. |
| Opportunité | 3 |

| M.PIEGE-ORGA | |
|---|---|
| Méthode d'attaque | 26 - PIÉGEAGE DU LOGICIEL |
| Description | Un utilisateur piège involontairement un logiciel du fait de :<br>- l'absence d'identification des biens sensibles,<br>- l'absence de contrôle des biens sensibles,<br>- l'absence de conservation et d'analyse des traces des activités,<br>- l'absence de politique de protection des postes de travail,<br>- l'absence de politique globale de lutte contre le code malveillant. |
| Opportunité | 4 |

| M.DISPO-SUP | |
|---|---|
| Méthode d'attaque | 42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL |
| Description | L'atteinte à la disponibilité du personnel est aggravé par l'absence de procédures d'archivage des données contenues sur des supports (papier, magnétique). |
| Opportunité | 2 |

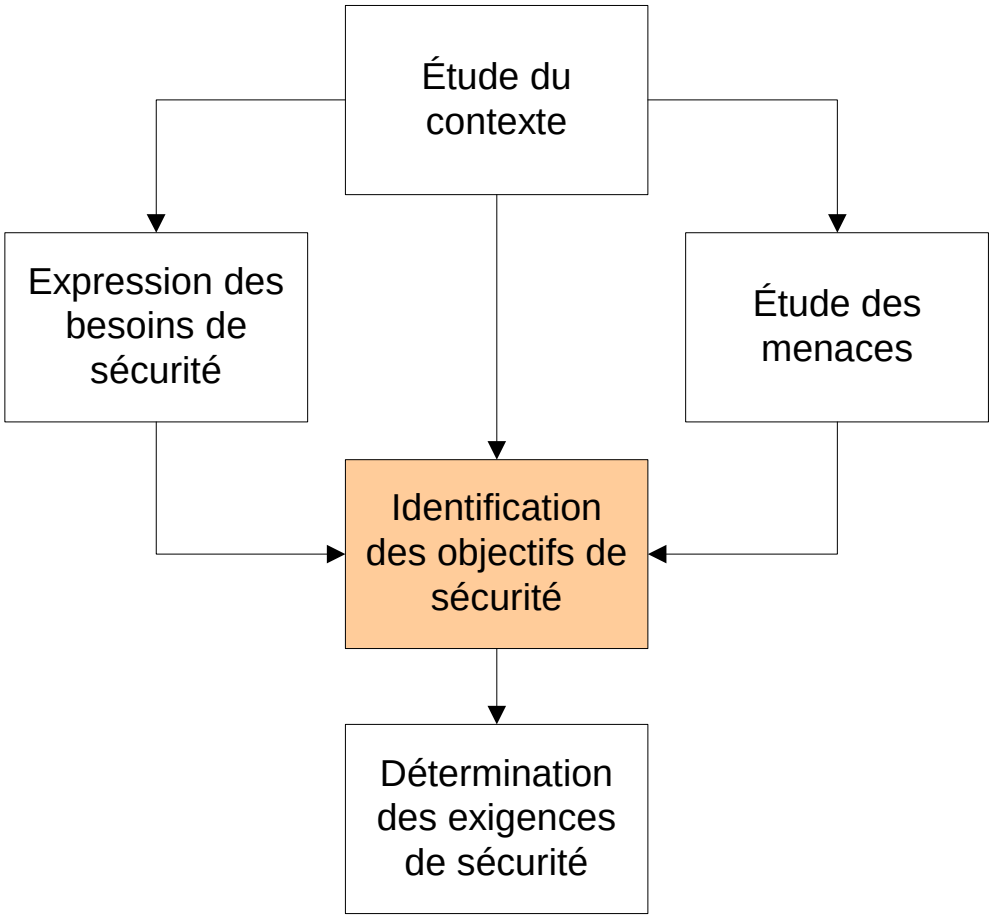
| M.DISPO-PER | |
|---|---|
| Méthode d'attaque | 42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL |
| Description | Le personnel est indisponible du fait de la maladie, de l'absentéisme ou d'un enjeu concurrentiel.<br><br>L'indisponibilité du personnel est aggravée par l'absence de procédures de transfert de connaissances. |
| Opportunité | 3 |

| M.DISPO-ORGA | |
|---|---|
| Méthode d'attaque | 42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL |
| Description | L'atteinte à la disponibilité du personnel est aggravée par des lacunes touchant l'organisation :<br>- absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles,<br>- absence de processus de gestion de la continuité des activités professionnelles de l'organisme,<br>- absence de procédures de transfert de connaissances,<br>- présence d'épidémie virale locale. |
| Opportunité | 4 |

Le tableau suivant présente la synthèse des menaces :

| | Confidentialité | Disponibilité | Intégrité | Opportunité | Potentiel d'attaque |
|---|---|---|---|---|---|
| M.ECOUTE-ORGA | X | | | 4 | 2 |
| M.ECOUTE-SITE | X | | | 4 | 2 |
| M.INCENDIE-LOG | | X | X | 4 | 2 |
| M.INCENDIE-PER | | X | X | 4 | 2 |
| M.INCENDIE-SITE | | X | X | 4 | 2 |
| M.PIEGE-LOG | X | X | X | 4 | 2 |
| M.PIEGE-MAT | X | X | X | 4 | 2 |
| M.PIEGE-ORGA | X | X | X | 4 | 2 |
| M.PIEGE-SUP | X | X | X | 4 | 2 |
| M.VOL-DOC-ORGA | X | | | 4 | 2 |
| M.VOL-DOC-SITE | X | | | 4 | 2 |
| M.VOL-MAT-SITE | X | X | | 4 | 2 |
| M.VOL-MAT-ORGA | X | X | | 4 | 2 |
| M.VOL-DOC-SUPPORT | X | | | 4 | 2 |
| M.DISPO-ORGA | | X | | 4 | 1 |
| M.DIV-PHY | X | | | 4 | 1 |
| M.DIV-ORGA | X | | | 4 | 1 |
| M.DIV-SUP | X | | | 4 | 1 |
| M.TELECOM-PHY | | X | | 4 | 1 |
| M.ECOUTE-PER | X | | | 3 | 2 |
| M.ICENDIE-MAT-FIXE | | X | X | 3 | 2 |
| M.VOL-DOC-PER | X | | | 3 | 2 |
| M.INCENDIE-ORGA | | X | X | 3 | 2 |
| M.ECOUTE-LOG | X | | | 3 | 2 |
| M.VOL-MAT-MAT | X | X | | 3 | 2 |
| M.ECOUTE-PHY | X | | | 3 | 2 |
| M.VOL-MAT-PER | X | X | | 3 | 2 |
| M.PIEGE-PER | X | X | X | 3 | 2 |
| M.DISPO-PER | | X | | 3 | 1 |
| M.DIV-PER | X | | | 3 | 1 |
| M.DIV-LOG | X | | | 3 | 1 |
| M.TELECOM-ORGA | | X | | 3 | 1 |
| M.TELECOM-PER | | X | | 3 | 1 |
| M.DIV-MAT | X | | | 3 | 1 |
| M.INCENDIE-SUPPORT | | X | X | 2 | 2 |
| M.ECOUTE-RES | X | | | 2 | 2 |
| M.INCENDIE-PHY | | X | X | 2 | 2 |
| M.DISPO-SUP | | X | | 2 | 1 |
| M.VOL-DOC-MAT | X | | | 1 | 2 |

# 6 Étape 4 : Identification des objectifs de sécurité




*D'une part, nous avons formalisé l'expression des besoins de sécurité, qui caractérisent ce que veut protéger l'organisme.*
*D'autre part, nous avons identifié les menaces qui pèsent sur l'organisme.*
*Nous allons maintenant déterminer la possibilité pour les menaces identifiées d'affecter réellement les éléments essentiels et d'impacter l'organisme. Il s'agit des risques.*

*L'ensemble des risques, des hypothèses et des règles de sécurité devra être parfaitement couvert par des objectifs de sécurité, en tenant compte des contraintes et autres éléments du contexte. Ils expriment ce que doit réaliser la cible pour que son système fonctionne de manière sécurisée.*

## 6.1 Activité 1 : Confrontation des menaces aux besoins

*À l'aide des besoins de sécurité exprimés pour chaque élément essentiel (en termes de disponibilité, intégrité, confidentialité…) et des menaces que nous venons de mettre en évidence (dont l'atteinte est aussi qualifiée selon leur méthode d'attaque en termes de disponibilité, intégrité, confidentialité), nous pouvons déterminer les besoins de sécurité qui peuvent être concernés, ce qui reflète un impact d'une menace sur l'organisme. Les besoins de sécurité concernés sont déterminés par méthode d'attaque et pour chaque élément essentiel. Ils se reporteront sur tous les risques comportant ces méthodes d'attaque.*
*Chaque besoin de sécurité concerné représente une possibilité pour l'organisme d'être impacté. Par conséquent, plus une menace est susceptible d'empêcher le respect des besoins de sécurité, plus l'impact peut être important pour l'organisme. C'est la raison pour laquelle on peut hiérarchiser les risques selon la somme des besoins de sécurité concernés.*

*Par ailleurs, il est intéressant de mettre en évidence les opportunités des menaces impliquées dans les risques. En effet, elles peuvent aussi aider à déterminer des priorités et à écarter des risques (il conviendra de justifier cette action).*

*Enfin, il convient de porter une grande attention à la rédaction des risques. Elle doit être claire, pratique, adaptée au contexte et qui doit comprendre, dans la mesure du possible, la description de la menace et les impacts sur l'organisme.*

### 6.1.1 Évaluation des risques

Voici un exemple du rapprochement des menaces aux besoins de sécurité pour un élément essentiel :

**I.VISU**

| | Confidentialité | Disponibilité | Intégrité | Confidentialité | Disponibilité | Intégrité |
|---|---|---|---|---|---|---|
| 01- INCENDIE | | X | X | | 2 | 2 |
| 13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION | | X | | | 2 | |
| 19 - ÉCOUTE PASSIVE | X | | | 0 | | |
| 20 - VOL DE SUPPORTS OU DE DOCUMENTS | X | | | 0 | | |
| 21 - VOL DE MATÉRIELS | X | X | | 0 | 2 | |
| 23 - DIVULGATION | X | | | 0 | | |
| 26 - PIÉGEAGE DU LOGICIEL | X | X | X | 0 | 2 | 2 |
| 42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL | | X | | | 2 | |

En faisant de même pour tous les éléments essentiels, nous obtenons les valeurs suivantes :

| | | F.CONTX | F.CPTA | F.DEVIS | F.PLAN | F.PROJET | F.STRUC | F.VISU | I.CDC | I.CONTRAT | I.CONTX | I.DEVIS | I.DOSS | I.FACT | I.PARA | I.PLAN | I.STRUC | I.TECH | I.VISU | Max. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M.DISPO-ORGA | Confidentialité | | | | | | | | | | | | | | | | | | | **3** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.DISPO-PER | Confidentialité | | | | | | | | | | | | | | | | | | | **3** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.DISPO-SUP | Confidentialité | | | | | | | | | | | | | | | | | | | **3** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.DIV-LOG | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.DIV-MAT | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.DIV-ORGA | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.DIV-PER | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.DIV-PHY | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.DIV-SUP | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.ECOUTE-LOG | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.ECOUTE-ORGA | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.ECOUTE-PER | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |

| | | F.CONTX | F.CPTA | F.DEVIS | F.PLAN | F.PROJET | F.STRUC | F.VISU | I.CDC | I.CONTRAT | I.CONTX | I.DEVIS | I.DOSS | I.FACT | I.PARA | I.PLAN | I.STRUC | I.TECH | I.VISU | Max. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M.ECOUTE-PHY | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.ECOUTE-RES | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.ECOUTE-SITE | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.ICENDIE-MAT-FIXE | Confidentialité | | | | | | | | | | | | | | | | | | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.INCENDIE-LOG | Confidentialité | | | | | | | | | | | | | | | | | | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.INCENDIE-ORGA | Confidentialité | | | | | | | | | | | | | | | | | | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.INCENDIE-PER | Confidentialité | | | | | | | | | | | | | | | | | | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.INCENDIE-PHY | Confidentialité | | | | | | | | | | | | | | | | | | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.INCENDIE-SITE | Confidentialité | | | | | | | | | | | | | | | | | | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.INCENDIE-SUPPORT | Confidentialité | | | | | | | | | | | | | | | | | | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.PIEGE-LOG | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.PIEGE-MAT | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.PIEGE-ORGA | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |

| | | F.CONTX | F.CPTA | F.DEVIS | F.PLAN | F.PROJET | F.STRUC | F.VISU | I.CDC | I.CONTRAT | I.CONTX | I.DEVIS | I.DOSS | I.FACT | I.PARA | I.PLAN | I.STRUC | I.TECH | I.VISU | Max. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.PIEGE-PER | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.PIEGE-SUP | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **4** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | 4 | 4 | 4 | 4 | 2 | 4 | 2 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 4 | 2 | |
| M.TELECOM-ORGA | Confidentialité | | | | | | | | | | | | | | | | | | | **3** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.TELECOM-PER | Confidentialité | | | | | | | | | | | | | | | | | | | **3** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.TELECOM-PHY | Confidentialité | | | | | | | | | | | | | | | | | | | **3** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.VOL-DOC-MAT | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.VOL-DOC-ORGA | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.VOL-DOC-PER | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.VOL-DOC-SITE | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.VOL-DOC-SUPPORT | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **2** |
| | Disponibilité | | | | | | | | | | | | | | | | | | | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.VOL-MAT-MAT | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **3** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.VOL-MAT-ORGA | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **3** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.VOL-MAT-PER | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **3** |

| | | F.CONTX | F.CPTA | F.DEVIS | F.PLAN | F.PROJET | F.STRUC | F.VISU | I.CDC | I.CONTRAT | I.CONTX | I.DEVIS | I.DOSS | I.FACT | I.PARA | I.PLAN | I.STRUC | I.TECH | I.VISU | Max. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |
| M.VOL-MAT-SITE | Confidentialité | | | | | | | | 1 | 1 | 1 | 1 | 1 | 1 | 2 | | | 2 | | **3** |
| | Disponibilité | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | |
| | Intégrité | | | | | | | | | | | | | | | | | | | |

Rappelons les impacts sur l'organisme ; ils peuvent survenir dès lors qu'un besoin de sécurité n'est pas respecté :

| **Impacts** | **Exemples** |
|---|---|
| Perte d'image de marque | Mauvaise presse<br>Bouche à oreille négatif<br>Utilisation par la concurrence |
| Infraction aux lois, aux règlements | Action de justice à l'encontre du cabinet<br>Non respect de la réglementation métier |
| Perte d'un avantage concurrentiel | Perte d'un savoir-faire métier<br>Vol d'un savoir-faire métier |

Voici les conclusions que nous tirons de l'exploitation de la synthèse des besoins de sécurité touchés :

- les risques reposant sur les méthodes d'attaque relatives à l'incendie et au piégeage de logiciel sont susceptibles de porter atteinte à un grand nombre de besoins de sécurité dont la valeur maximale est 4 ; il s'agit donc des risques dont il est très important de se prémunir, et de manière prioritaire ;

- les risques reposant sur les méthodes d'attaque relatives à la perte des moyens de télécommunication, au vol de matériel et à l'atteinte à la disponibilité des personnels peuvent porter atteinte à un nombre important de besoins de sécurité dont la valeur maximale est 3 ; il s'agit donc de risques dont il est important de se prémunir ;

- les risques reposant sur les autres méthodes d'attaque sont moins importants ; il apparaît donc comme moins prioritaire de s'en prémunir.

### 6.1.2 Synthèse des risques

Le tableau suivant présente la liste des 39 risques auxquels le cabinet d'études est exposé.

| R.DISPO-ORGA | |
|---|---|
| Libellé | R.DISPO-ORGA |
| Méthode d'attaque | 42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL |
| Description | L'atteinte à la disponibilité du personnel est aggravée par des lacunes touchant l'organisation :<br>- absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles,<br>- absence de processus de gestion de la continuité des activités professionnelles de l'organisme,<br>- absence de procédures de transfert de connaissances,<br>- présence d'épidémie virale locale.<br><br>Cela peut affecter la disponibilité de tous les éléments essentiels (notamment les éléments essentiels F.PLAN, I.DOSS, I.TECH ayant besoin d'une disponibilité temps réel), entraînant une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.DISPO-PER | |
|---|---|
| Libellé | R.DISPO-PER |
| Méthode d'attaque | 42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL |
| Description | Le personnel est indisponible du fait de la maladie, de l'absentéisme ou d'un enjeu concurrentiel.<br><br>L'indisponibilité du personnel est aggravée par l'absence de procédures de transfert de connaissances.<br><br>Cela peut porter atteinte à la disponibilité de tous les éléments essentiels (notamment F.PLAN ayant un besoin de disponibilité en temps réel, et I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée), entraînant une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.DISPO-SUP | |
|---|---|
| Libellé | R.DISPO-SUP |
| Méthode d'attaque | 42 - ATTEINTE À LA DISPONIBILITÉ DU PERSONNEL |
| Description | L'atteinte à la disponibilité du personnel est aggravée par l'absence de procédures d'archivage des données contenues sur des supports (papier, magnétique).<br><br>Cela peut porter atteinte à la disponibilité de tous les éléments essentiels (notamment F.PLAN, I.DOSS, ITECH ayant un besoin de disponibilité dans la journée) |
| Opportunité | 2 |

| R.DIV-LOG | |
|---|---|
| Libellé | R.DIV-LOG |
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne du cabinet d'études qui, par négligence, du fait de l'absence de vérification des accès partagés accordés au niveau logiciel, diffuse de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître.<br><br>L'absence de vérification des accès partagés accordés au niveau logiciel peut porter atteinte à la confidentialité de toutes les informations (notamment I.PARA et I.TECH ayant un besoin de confidentialité restreint à une équipe projet) entraînant une perte d'image de marque ou d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.DIV-MAT | |
|---|---|
| Libellé | R.DIV-MAT |
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne du cabinet d'études, diffuse par négligence de l'information à d'autres personnes de l'organisme n'ayant pas le besoin d'en connaître ou à l'extérieur du fait de l'absence de vérification des accès partagés accordés aux fonctions de gestion des droits d'accès trop compliquées à utiliser et pouvant être source d'erreur ou de la présence de répertoires partagés pour stocker de l'information.<br><br>Elle porte atteinte à la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br>Cela peut engendrer une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.DIV-ORGA | |
|---|---|
| Libellé | R.DIV-ORGA |
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne du cabinet d'études diffuse des informations de façon involontaire ou délibérée, du fait de la présence de vulnérabilités dans l'organisation :<br>- absence d'identification des biens sensibles,<br>- absence d'organisation responsable de la définition, de la mise en oeuvre et du contrôle des privilèges d'accès à l'information,<br>- absence de contrôle des biens sensibles,<br>- absence de politique de protection de l'information,<br>- la politique de sécurité n'est pas appliquée,<br>- les responsables sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous.<br><br>Elle porte atteinte à la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br>Cela peut engendrer une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

**R.DIV-PER**

| | |
|---|---|
| Libellé | R.DIV-PER |
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne du cabinet d'études divulgue de façon délibérée ou non des renseignements du fait du non-respect des règles de classification de l'information ou de l'absence de sensibilisation à la protection de l'information à caractère sensible et de soutien de la direction à l'application de la politique de sécurité vis-à-vis du personnel.<br><br>Elle porte atteinte à la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br><br>Cela peut engendrer une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 3 |

**R.DIV-PHY**

| | |
|---|---|
| Libellé | R.DIV-PHY |
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne du cabinet d'études diffuse de façon délibérée ou non des informations du fait de l'absence de contrôle des échanges avec l'extérieur.<br><br>Elle affecte la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br><br>Cela peut entraîner une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

**R.DIV-SUP**

| | |
|---|---|
| Libellé | R.DIV-SUP |
| Méthode d'attaque | 23 - DIVULGATION |
| Description | Une personne du cabinet d'études divulgue de façon délibérée ou non des informations, grâce à l'utilisation de supports capables d'effectuer des échanges d'information à caractère sensible (papier, clé USB, disquette...).<br><br>Elle porte atteinte à la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br><br>Elle peut avoir pour conséquences une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.ECOUTE-LOG | |
|---|---|
| Libellé | R.ECOUTE-LOG |
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Un attaquant utilisant les équipements ou supports de communication exploite les caractéristiques logiciel suivantes pour faire de l'écoute passive :<br>- absence de dispositif de contrôle accès en cas d'inactivité,<br>- absence de protection des journaux récoltant la trace des activités,<br>- absence de protection contre l'usage de privilèges avancés,<br>- pas de changement de mot de passe d'accès,<br>- possibilité d'ajout d'un logiciel d'écoute de type cheval de Troie.<br><br>Il affecte la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br>Cela peut engendrer une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.ECOUTE-ORGA | |
|---|---|
| Libellé | R.ECOUTE-ORGA |
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Un attaquant connecté au réseau exerce une écoute passive en profitant :<br>- de l'absence d'identification des biens sensibles,<br>- de l'absence de contrôle de l'application de la politique de sécurité,<br>- de la politique de sécurité n'est pas appliquée,<br>- du fait que les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées.<br><br>Il porte atteinte à la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br>Cela peut engendrer une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.ECOUTE-PER | |
|---|---|
| Libellé | R.ECOUTE-PER |
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Une personne malveillante directement connectée au réseau exploite la faible sensibilisation à la protection en confidentialité des échanges d'information, l'absence de soutien de la direction à l'application de la politique de sécurité ou le manque de formation du personnel aux mesures et outils de protection des échanges externe et interne, pour exercer une écoute passive.<br><br>Elle touche à la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br>Cela peut engendrer une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.ECOUTE-PHY | |
|---|---|
| Libellé | R.ECOUTE-PHY |
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Un intervenant extérieur, un concurrent ou une personne interne malveillante exerce une écoute passive grâce à l'absence de protection d'accès au modem ADSL et au central téléphonique.<br><br>Elle porte atteinte à la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br><br>Cela engendre une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.ECOUTE-RES | |
|---|---|
| Libellé | R.ECOUTE-RES |
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Un concurrent, un intervenant extérieur ou une personne malveillante, utilise un médium (Téléphone, ADSL, câble Ethernet) permettant la pose de matériel d'écoute pour exercer une écoute passive.<br><br>Il porte atteinte à la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br><br>Cela peut engendrer une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 2 |

| R.ECOUTE-SITE | |
|---|---|
| Libellé | R.ECOUTE-SITE |
| Méthode d'attaque | 19 - ÉCOUTE PASSIVE |
| Description | Un concurrent, un intervenant extérieur ou une personne interne malveillante profite de l'absence de contrôle d'accès au site pour entrer dans les locaux afin d'exercer une écoute passive.<br><br>Il porte atteinte à la confidentialité des informations suivantes :<br>- I.CONTRAT, I.CDC, I.DEVIS, I.DOSS, I.FACT (Confidentialité restreinte au cabinet et aux clients ),<br>- I.PARA, I.TECH (Confidentialité restreinte au cabinet).<br><br>Cela peut engendrer une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.ICENDIE-MAT-FIXE | |
|---|---|
| Libellé | R.ICENDIE-MAT-FIXE |
| Méthode d'attaque | 01- INCENDIE |
| Description | Un incendie accidentel (dû à la foudre ou à un court-circuit sur un produit inflammable) est aggravé par l'absence de matériels fixes de remplacement et du stockage de matériaux inflammables.<br><br>Une personne malveillante utilise des matériaux inflammables présents au sein de l'entreprise pour déclencher un incendie.<br><br>Il affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Il porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.PROJET, F.DEVIS, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.INCENDIE-LOG | |
|---|---|
| Libellé | R.INCENDIE-LOG |
| Méthode d'attaque | 01- INCENDIE |
| Description | Un incendie ayant une origine accidentelle (un court circuit ou la foudre) ou volontaire (un terroriste ou un concurrent malveillant), est aggravé du fait de l'unicité des exemplaires des contrats de licence des logiciels.<br><br>Il affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Il porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.PROJET, F.DEVIS, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.INCENDIE-ORGA | |
|---|---|
| Libellé | R.INCENDIE-ORGA |
| Méthode d'attaque | 01- INCENDIE |
| Description | Un incendie déclenché de façon volontaire (un terroriste ou un concurrent) ou par accident (foudre, court-circuit) est aggravé par l'absence :<br>- de procédures de sauvegarde des donnés contenues sur les supports,<br>- d'organisation de lutte contre l'incendie,<br>- d'affichage des informations à jour pour l'appel des services d'urgence.<br><br>Il affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Il porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.PROJET, F.DEVIS, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.INCENDIE-PER | |
|---|---|
| Libellé | R.INCENDIE-PER |
| Méthode d'attaque | 01- INCENDIE |
| Description | Un incendie dû à un évènement intentionnel (un terroriste, un concurrent) ou accidentel (la foudre, un court-circuit) est aggravé compte tenu de l'absence de test des procédures de réaction et d'information, ainsi que par la méconnaissance des mesures de sécurité de la part du personnel.<br><br>Il affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Il porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.PROJET, F.DEVIS, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.INCENDIE-PHY | |
|---|---|
| Libellé | R.INCENDIE-PHY |
| Méthode d'attaque | 01- INCENDIE |
| Description | Aggravation des conséquences d'un incendie accidentel ou délibéré, à cause de l'absence de prise en compte des risques d'incendie dans la phase d'installation du central téléphonique et du réseau électrique.<br><br>Il affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Il porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.PROJET, F.DEVIS, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 2 |

| R.INCENDIE-SITE | |
|---|---|
| Libellé | R.INCENDIE-SITE |
| Méthode d'attaque | 01- INCENDIE |
| Description | Un terroriste ou un concurrent profite de la présence d'ouverture sur la voie publique ainsi que les absences de cloisonnement anti-feu et de contrôle d'accès au sein du site pour déclencher un incendie.<br><br>Il affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Elle porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.PROJET, F.DEVIS, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.INCENDIE-SUPPORT | |
|---|---|
| Libellé | R.INCENDIE-SUPPORT |
| Méthode d'attaque | 01- INCENDIE |
| Description | Un incendie causé de façon accidentelle (la foudre, un court-circuit) ou intentionnelle (un terroriste ou un concurrent) est aggravé par l'absence de sauvegarde des données contenues sur le matériel transportable.<br><br>Il affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Il porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.PROJET, F.DEVIS, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 2 |

| R.PIEGE-LOG | |
|---|---|
| Libellé | R.PIEGE-LOG |
| Méthode d'attaque | 26 - PIÉGEAGE DU LOGICIEL |
| Description | Une personne introduit de façon involontaire (une personne interne exécutant à son insu un virus) un logiciel ou des commandes de manière à modifier le comportement d'un logiciel grâce à l'absence de protection contre l'usage de privilèges avancés ou de mise en oeuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels.<br><br>Elle touche la confidentialité de certaines informations :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT ayant un besoin en confidentialité restreint au cabinet et aux clients.<br><br>Elle affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Elle porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.DEVIS, F.PROJET, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.PIEGE-MAT | |
|---|---|
| Libellé | R.PIEGE-MAT |
| Méthode d'attaque | 26 - PIÉGEAGE DU LOGICIEL |
| Description | Un utilisateur légitime du système d'information amorce involontairement un matériel à partir d'un périphérique.<br><br>Il touche la confidentialité de certaines informations :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT ayant un besoin en confidentialité restreint au cabinet et aux clients.<br><br>Elle affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Elle porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.DEVIS, F.PROJET, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.PIEGE-ORGA | |
|---|---|
| Libellé | R.PIEGE-ORGA |
| Méthode d'attaque | 26 - PIÉGEAGE DU LOGICIEL |
| Description | Un utilisateur piège involontairement un logiciel du fait de :<br>- l'absence d'identification des biens sensibles,<br>- l'absence de contrôle des biens sensibles,<br>- l'absence de conservation et d'analyse des traces des activités,<br>- l'absence de politique de protection des postes de travail,<br>- l'absence de politique globale de lutte contre le code malveillant.<br><br>Il touche la confidentialité de certaines informations :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT ayant un besoin en confidentialité restreint au cabinet et aux clients.<br><br>Elle affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Il porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.DEVIS, F.PROJET, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.PIEGE-PER | |
|---|---|
| Libellé | R.PIEGE-PER |
| Méthode d'attaque | 26 - PIÉGEAGE DU LOGICIEL |
| Description | Un utilisateur piège involontairement un logiciel du fait :<br>- du manque de sensibilisation à la menace des codes malveillant,<br>- de la méconnaissance des procédures d'intervention et de réactions réflexes en cas de détection d'anomalie,<br>- du non-respect des règles de mises à jour des logiciels anti-virus, vis-à-vis du personnel.<br><br>Il touche à la confidentialité de certaines informations :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT ayant un besoin en confidentialité restreint au cabinet et aux clients.<br><br>Elle affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Il porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.DEVIS, F.PROJET, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.PIEGE-SUP | |
|---|---|
| Libellé | R.PIEGE-SUP |
| Méthode d'attaque | 26 - PIÉGEAGE DU LOGICIEL |
| Description | Un utilisateur piège un logiciel du fait de l'absence de moyens permettant le contrôle d'innocuité des supports magnétiques (clé USB, disquette) lors de leurs entrées dans l'organisme.<br><br>Il touche à la confidentialité de certaines informations :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT ayant un besoin en confidentialité restreint au cabinet et aux clients.<br><br>Elle affecte la disponibilité de tous les éléments essentiels, notamment F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée.<br><br>Il porte atteinte également à l'intégrité de tous les éléments essentiels, notamment :<br>- F.CONTX, F.CPTA, F.PLAN, F.STRUCT, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.TECH ayant un besoin en intégrité fort,<br>- F.DEVIS, F.PROJET, F.VISU, I.VISU ayant un besoin en intégrité moyen.<br><br>Cela peut engendrer une infraction aux lois ainsi qu'une perte d'image de marque et d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.TELECOM-ORGA | |
|---|---|
| Libellé | R.TELECOM-ORGA |
| Méthode d'attaque | 13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION |
| Description | L'absence de maintenance des terminaux téléphoniques et Internet de la part de l'organisation aggrave la perte des moyens de télécommunication.<br><br>Elle peut affecter la disponibilité de tous les éléments essentiels (notamment les éléments essentiels F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée), entraînant une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.TELECOM-PER | |
|---|---|
| Libellé | R.TELECOM-PER |
| Méthode d'attaque | 13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION |
| Description | Un attaquant accédant aux dispositifs de télécommunication profite de la méconnaissance du personnel concernant les mesures de sécurité pour entraîner une perte des moyens de télécommunication.<br><br>Elle peut affecter la disponibilité de tous les éléments essentiels (notamment les éléments essentiels F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée), entraînant une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.TELECOM-PHY | |
|---|---|
| Libellé | R.TELECOM-PHY |
| Méthode d'attaque | 13 - PERTE DES MOYENS DE TÉLÉCOMMUNICATION |
| Description | La perturbation, l'arrêt ou le mauvais dimensionnement des services de télécommunication entraîne une perte des moyens de télécommunications de manière accidentelle à cause :<br>- d'un dysfonctionnement des réseaux externes,<br>- d'un défaut d'exploitation du réseau téléphonique interne,<br>- de l'absence de la maintenance des équipements de télécommunication,<br>- de l'absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service d'accès à Internet ou téléphonique.<br><br>Un concurrent exploite le fait que l'accès physique des locaux hébergeant les moyens de télécommunication ne soit pas protégé pour attaquer les moyens de télécommunication.<br><br>Elle peut affecter la disponibilité de tous les éléments essentiels (notamment les éléments essentiels F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée), entraînant une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.VOL-DOC-MAT | |
|---|---|
| Libellé | R.VOL-DOC-MAT |
| Méthode d'attaque | 20 - VOL DE SUPPORTS OU DE DOCUMENTS |
| Description | Une personne malveillante, un concurrent ou une personne interne à l'organisme profite de l'absence d'inventaire du matériel, des disques durs facilement démontables ou de la présence de matériels attractifs, pour voler un support ou un document.<br><br>Elle porte atteinte à la confidentialité de certaines informations, notamment :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOS, I.FACT ayant un besoin en confidentialité restreint au cabinet et aux clients.<br>Cela peut entraîner une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 1 |

| R.VOL-DOC-ORGA | |
|---|---|
| Libellé | R.VOL-DOC-ORGA |
| Méthode d'attaque | 20 - VOL DE SUPPORTS OU DE DOCUMENTS |
| Description | Une personne interne à l'organisme ou extérieure effectue un vol de supports ou de documents en exploitant l'une des vulnérabilités de l'organisation suivante :<br>- absence d'identification des biens sensibles,<br>- absence d'organisation de gestion des incidents de sécurité,<br>- absence de contrôle de l'application de la politique de sécurité,<br>- absence de contrôle des biens sensibles,<br>- la politique de sécurité n'est pas appliquée,<br>- les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous.<br><br>Elle porte atteinte à la confidentialité de certaines informations, notamment :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOS, I.FACT ayant un besoin en confidentialité restreint au cabinet et aux clients.<br>Cela peut entraîner une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.VOL-DOC-PER | |
|---|---|
| Libellé | R.VOL-DOC-PER |
| Méthode d'attaque | 20 - VOL DE SUPPORTS OU DE DOCUMENTS |
| Description | Une personne interne à l'organisme, ou un intervenant externe vole un document ou un support en profitant de l'absence de sensibilisation à la protection des documents à caractère confidentiel ou du non respect des règles associées à la classification des informations de la part du personnel.<br><br>Elle porte atteinte à la confidentialité de certaines informations, notamment :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOS, I.FACT ayant un besoin en confidentialité restreint au cabinet et aux clients.<br>Cela peut entraîner une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.VOL-DOC-SITE | |
|---|---|
| Libellé | R.VOL-DOC-SITE |
| Méthode d'attaque | 20 - VOL DE SUPPORTS OU DE DOCUMENTS |
| Description | Une personne externe s'introduit dans l'organisme pour voler des supports ou des documents, profitant de l'absence de contrôle d'accès au site.<br><br>Elle porte atteinte à la confidentialité de certaines informations, notamment :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOS, I.FACT ayant un besoin en confidentialité restreint au cabinet et aux clients.<br>Cela peut entraîner une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.VOL-DOC-SUPPORT | |
|---|---|
| Libellé | R.VOL-DOC-SUPPORT |
| Méthode d'attaque | 20 - VOL DE SUPPORTS OU DE DOCUMENTS |
| Description | Une personne malveillante effectue un vol de documents exploitant le fait que les supports soient accessibles par tous et aisément transportables.<br>Une personne interne ou externe à l'organisme effectue un vol de documents, profitant de l'absence d'inventaire ou de protection des supports.<br>Un vol de documents ou de support par une personne interne ou externe à l'organisme est aggravé par l'utilisation de supports originaux non sauvegardés.<br><br>Elle porte atteinte à la confidentialité de certaines informations, notamment :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOS, I.FACT ayant un besoin en confidentialité restreint au cabinet et aux clients.<br>Elle peut entraîner une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.VOL-MAT-MAT | |
|---|---|
| Libellé | R.VOL-MAT-MAT |
| Méthode d'attaque | 21 - VOL DE MATÉRIELS |
| Description | Une personne interne ou externe à l'organisme vole des matériels du fait de l'utilisation de matériels attractifs, démontables ou de l'absence d'inventaire.<br>Le vol de matériels par une personne interne ou externe à l'organisme est aggravé par l'absence de matériel de remplacement.<br><br>Il porte atteinte à la confidentialité de certaines informations :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet et aux clients,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT ayant un besoin en confidentialité restreint au cabinet.<br>Il affecte la disponibilité de tous les éléments essentiels :<br>- F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée,<br>- F.CONTX, F.DEVIS, F.PROJET, F.STRUCT, F.VISU, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.VISU ayant un besoin en disponibilité dans la semaine.<br>Cela peut avoir pour conséquences une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.VOL-MAT-ORGA | |
|---|---|
| Libellé | R.VOL-MAT-ORGA |
| Méthode d'attaque | 21 - VOL DE MATÉRIELS |
| Description | Un vol de matériels par une personne externe ou interne à l'organisme est aggravé par l'absence d'identification des biens sensibles ou de gestion des incidents de sécurité lié au vol.<br><br>Une personne interne ou externe à l'organisme exploite l'absence de contrôle de l'application de la politique de sécurité pour effectuer un vol de matériel.<br><br>Un personne externe utilise les entrées/sorties des matériels dans l'organisation pour effectuer un vol de matériel.<br><br>Elle porte atteinte à la confidentialité de certaines informations :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet et aux clients,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT ayant un besoin en confidentialité restreint au cabinet.<br><br>Elle affecte la disponibilité de tous les éléments essentiels :<br>- F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée,<br>- F.CONTX, F.DEVIS, F.PROJET, F.STRUCT, F.VISU, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.VISU ayant un besoin en disponibilité dans la semaine.<br><br>Cela peut avoir pour conséquences une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 4 |

| R.VOL-MAT-PER | |
|---|---|
| Libellé | R.VOL-MAT-PER |
| Méthode d'attaque | 21 - VOL DE MATÉRIELS |
| Description | Une personne externe à l'organisme vole du matériel en exploitant l'absence de soutien de la direction à l'application de la politique de sécurité, la faible sensibilisation à la protection des matériels en dehors de l'organisme ou le non-respect des règles de protection des équipements transportables de la part du personnel.<br><br>Elle porte atteinte à la confidentialité de certaines informations :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet et aux clients,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT ayant un besoin en confidentialité restreint au cabinet.<br><br>Elle affecte la disponibilité de tous les éléments essentiels :<br>- F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée,<br>- F.CONTX, F.DEVIS, F.PROJET, F.STRUCT, F.VISU, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.VISU ayant un besoin en disponibilité dans la semaine.<br><br>Cela peut avoir pour conséquences une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 3 |

| R.VOL-MAT-SITE | |
|---|---|
| Libellé | R.VOL-MAT-SITE |
| Méthode d'attaque | 21 - VOL DE MATÉRIELS |
| Description | Une personne externe, profitant de l'absence de contrôle d'accès au site, s'infiltre au sein de l'organisme et vole des matériels.<br><br>Elle porte atteinte à la confidentialité de certaines informations :<br>- I.PARA, I.TECH ayant un besoin en confidentialité restreint au cabinet et aux clients,<br>- I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.DOSS, I.FACT ayant un besoin en confidentialité restreint au cabinet.<br><br>Elle affecte la disponibilité de tous les éléments essentiels :<br>- F.PLAN, I.DOSS, I.TECH ayant un besoin en disponibilité dans la journée,<br>- F.CONTX, F.DEVIS, F.PROJET, F.STRUCT, F.VISU, I.CDC, I.CONTRAT, I.CONTX, I.DEVIS, I.FACT, I.PARA, I.PLAN, I.STRUC, I.VISU ayant un besoin en disponibilité dans la semaine.<br><br>Cela peut avoir pour conséquences une perte d'image de marque ou une perte d'un avantage concurrentiel. |
| Opportunité | 4 |

## 6.2 Activité 2 : Identification des objectifs de sécurité

*Les objectifs de sécurité doivent couvrir la totalité des risques, tout en tenant compte des hypothèses, des règles de sécurité et des différents éléments du contexte (les contraintes et enjeux notamment).*

*La complétude de cette couverture doit être démontrée en expliquant :*
- *comment les objectifs couvrent tous les risques et les règles de sécurité (et éventuellement les exigences réglementaires) ;*
- *que les objectifs sont pertinents vis-à-vis des hypothèses d'utilisation (et éventuellement des enjeux du système-cible) ;*
- *la nécessité de chaque objectif de sécurité.*

*La couverture peut être synthétisée par une valeur selon l'échelle suivante :*

| | |
|---|---|
| *0* | *Aucune couverture* |
| *1* | *Couverture faible* |
| *2* | *Couverture moyenne* |
| *3* | *Couverture importante* |
| *4* | *Couverture complète* |

*Il conviendra de mettre en évidence ce qui n'est pas couvert complètement (notamment les risques résiduels).*

*Pour les objectifs de sécurité destinés à couvrir des risques, on note qu'ils sont généralement exprimés sous la forme de vulnérabilités portées par des entités qu'il convient de contrer.*

*Ils constitueront ainsi un cahier des charges complet, ouvert (ne préjugeant pas des solutions à adopter) et parfaitement adapté à la problématique de l'organisme.*

### 6.2.1 Formalisation des objectifs de sécurité

La liste suivante présente les 52 objectifs de sécurité identifiés pour le cabinet d'études.

| **O.LOG-AUTH** | |
|---|---|
| Contenu | Tout accès aux systèmes doit être protégé par un dispositif d'identification et d'authentification |

| **O.LOG-CONF-SYS** | |
|---|---|
| Contenu | La configuration des systèmes et applications doit être conforme aux exigences de la politique de sécurité |

| **O.LOG-HABIL** | |
|---|---|
| Contenu | Il doit exister une gestion active des habilitations au sein des systèmes pour le traitement des informations en fonction des besoins d'en connaître et d'en modifier |

| **O.LOG-LICEN** | |
|---|---|
| Contenu | Il doit exister une gestion des licences, de leur enregistrement et de leur conservation |

| **O.MAT-AMOR** | |
|---|---|
| Contenu | Un utilisateur légitime du système d'information ne doit pas pouvoir amorcer involontairement un matériel à partir d'un périphérique. |

| O.MAT-AUTH-DOC | |
|---|---|
| Contenu | Les documents réalisés par le cabinet d'études doivent pouvoir être authentifiés |

| O.MAT-DESCR | |
|---|---|
| Contenu | La description de tous les équipements informatiques et leur localisation doivent être assurée en continu |

| O.MAT-DIV | |
|---|---|
| Contenu | Le cabinet d'études doit empêcher qu'une personne interne divulgue de façon délibérée ou non des informations, grâce à l'utilisation de supports capables d'effectuer des échanges d'information à caractère sensible (papier, clé USB, disquette...) et porte ainsi atteinte à la confidentialité des éléments essentiels. |

| O.MAT-ERG | |
|---|---|
| Contenu | L'ergonomie et la facilité de maintenance doivent être pris en compte dans le choix des matériels, supports et logiciels |

| O.MAT-PROT | |
|---|---|
| Contenu | Les équipements informatiques et les supports (cartouches de sauvegarde, disques durs, micro-ordinateurs portables) doivent être protégés contre les vols |

| O.MAT-REMP | |
|---|---|
| Contenu | Le matériel doit être remplacé ou remis en état dans les délais correspondant aux besoins exprimés. |

| O.MAT-RESTAU | |
|---|---|
| Contenu | Il doit être possible de restaurer tout ou une partie d'un système, d'une application, d'un ensemble de données et d'une trace en cas de sinistre, de panne ou de négligence |

| O.ORG-ARCHIV | |
|---|---|
| Contenu | Une politique d'archivage doit garantir la récupération intègre des données pendant toute la période fixée pour leur conservation |

| O.ORG-CONF | |
|---|---|
| Contenu | L'organisation doit s'assurer de l'identification du caractère confidentiel de toute information et s'assurer de l'application des règles de protection adéquates |

| O.ORG-CONSIGN | |
|---|---|
| Contenu | L'organisation doit s'assurer que les consignes de sécurité seront respectées en cas d'incident ou de malveillance |

| O.ORG-CONT-OBJ | |
|---|---|
| Contenu | L'organisation doit garantir le contrôle des mesures de sécurité et leur adéquation par rapport aux objectifs de sécurité |

| O.ORG-CRISE | |
|---|---|
| Contenu | L'organisation doit garantir une réaction rapide et efficace en cas de crise assurant une réduction des impacts potentiels et la continuité des activités essentielles : panne, sinistre, intrusion majeure, autre malveillance |

| O.ORG-EQMT | |
|---|---|
| Contenu | L'organisation doit intégrer une politique préventive contre la saturation et les pannes des équipements (informatiques, climatisation, énergie, communication) |

| O.ORG-EXIG | |
|---|---|
| Contenu | L'organisation doit garantir que les exigences minimales de sécurité des systèmes d'information sont respectées de tous |

| O.ORG-MAINTIEN | |
|---|---|
| Contenu | L'organisation doit s'assurer que tout matériel ou logiciel est maintenu |

| O.ORG-MOY | |
|---|---|
| Contenu | L'organisation doit garantir que les moyens de secours sont opérationnels et assurent si cela est possible la continuité de service des activités sensibles de l'organisme en cas de panne, de sinistre ou de malveillance majeure |

| O.ORG-POL-SYS | |
|---|---|
| Contenu | L'organisation doit garantir le respect de la politique de sécurité lors de la mise en place de tout système sensible (matériel ou logiciel) |

| O.ORG-POL-SYS-SENS | |
|---|---|
| Contenu | L'organisation doit faire respecter les exigences de la politique de sécurité dans le développement, l'usage et l'exploitation des systèmes (matériels et logiciels) |

| O.ORG-PREUV | |
|---|---|
| Contenu | L'organisation doit s'assurer que les traces et les éléments de preuves sont exploités et protégés en accord avec la politique de sécurité |

| O.ORG-PSSI | |
|---|---|
| Contenu | Le cabinet d'étude doit disposer d'une politique de sécurité des systèmes d'information (PSSI). |

| O.ORG-REGLEMENT | |
|---|---|
| Contenu | L'organisation doit s'assurer que l'ensemble des lois et règlements applicables sont pris en compte dans la politique de sécurité |

| O.ORG-ROLES | |
|---|---|
| Contenu | Chaque rôle lié à la sécurité du système d'information doit toujours (même en cas d'absence du titulaire) être placé sous la responsabilité d'au moins une personne ayant les compétences requises ou la possibilité de se référer à une documentation adéquate |

| O.ORG-SAUV | |
|---|---|
| Contenu | L'organisation doit s'assurer que toutes les données sont sauvegardées selon une fréquence adéquate (y compris des données non centralisées) |

| O.ORG-SSTRAIT | |
|---|---|
| Contenu | L'organisation doit s'assurer que ses sous-traitants/prestataires/fournisseurs/industriels/organisations filles/sites respectent la politique de sécurité lors de leurs interventions (travaux, développement, maintenance...) |

| O.ORG-SUIV-INCID | |
|---|---|
| Contenu | L'organisation doit assurer le traitement et le suivi de tout incident de sécurité identifié dans l'organisme |

| O.ORG-TRANS | |
|---|---|
| Contenu | Les moyens de transmission (selon leur nature) et leur exploitation doivent garantir la protection de leur contenu contre les risques de divulgation, de vol, d'altération, de répudiation et de perte |

| O.ORG-TRAV | |
|---|---|
| Contenu | L'organisation doit s'assurer que les conditions de travail sont satisfaisantes |

| O.ORG-VIRUS | |
|---|---|
| Contenu | La politique anti-virus doit empêcher l'introduction et la diffusion dans les systèmes de tout code malveillant |

| O.ORG-VOL | |
|---|---|
| Contenu | Les procédures d'entrées et sorties doivent lutter contre le vol des matériels |

| O.PER-ADHES | |
|---|---|
| Contenu | Le personnel doit adhérer à la démarche sécurité et les rôles et responsabilités doivent être clairs et connus |

| O.PER-IMP | |
|---|---|
| Contenu | L'implication de la direction dans la démarche sécurité doit être réelle et visible |

| O.PER-INCID | |
|---|---|
| Contenu | Le personnel doit montrer des réactions réflexes en cas d'incident (devoir d'information, moyens de remontée de l'information...) |

| O.PER-NORME | |
|---|---|
| Contenu | Le personnel doit être sensibilisé et formé au respect des normes de l'organisme |

| O.PER-POL | |
|---|---|
| Contenu | Les nouveaux personnels ou remplaçants doivent pouvoir assurer leurs tâches en respect de la politique de sécurité |

| O.PER-RESP | |
|---|---|
| Contenu | Le personnel doit être responsabilisé et informé des sanctions encourues |

| O.PER-SEC | |
|---|---|
| Contenu | Le personnel doit être sensibilisé au respect du secret professionnel et de la discrétion |

| O.PER-SENSIB | |
|---|---|
| Contenu | Les personnels ayant accès à des informations sensibles doivent être sensibilisés et identifiés |

| O.PER-USAGE | |
|---|---|
| Contenu | Les personnels doivent respecter les bons usages de l'outil informatique, des moyens de communication et de la manipulation des supports ainsi que les dispositions de sécurité associées à la classification des informations |

| O.PER-VOL | |
|---|---|
| Contenu | Les personnels doivent assurer à l'extérieur des locaux la protection contre le vol ou l'intrusion des équipements et supports |

| O.PER-VOLANT | |
|---|---|
| Contenu | Il doit exister un volant de personnel pour assurer la continuité des tâches en cas d'absence |

| O.PHY-ACCES | |
|---|---|
| Contenu | L'accès aux locaux du cabinet d'étude doit être contrôlé afin d'empêcher qu'un concurrent, un intervenant extérieur ou une personne interne exerce une écoute passive ou vol des supports, documents ou matériels. |

| O.PHY-INCEND | |
|---|---|
| Contenu | Les locaux doivent être protégés contre le déclenchement et la propagation d'incendies |

| O.PHY-MAT-DANG | |
|---|---|
| Contenu | Le stockage et la manipulation de matières ou de matériel potentiellement dangereux ne doivent pas induire de risques sur le système d'information |

| O.PHY-NORME | |
|---|---|
| Contenu | Le site doit être en conformité avec les normes de sécurité de l'organisme |

| O.RES-INT | |
|---|---|
| Contenu | Les accès aux interfaces de communication doivent être protégés contre une utilisation malveillante ou abusive |

| O.PHY-SERVICES | |
|---|---|
| Contenu | La fourniture des services essentiels au fonctionnement des matériels (i.e. électricité, communication, climatisation...) doit être assurée, de bonne qualité et si possible maîtrisée par l'organisme. |

| O.RES-TRANS | |
|---|---|
| Contenu | Les interfaces de communication doivent protéger les transmissions en confidentialité, intégrité et disponibilité |

### 6.2.2 Démonstration de la couverture

Les tableaux suivants présentent comment les objectifs de sécurité (il convient pour chacun de vérifier la compatibilité avec les contraintes pesant sur l'organisme et sur le système-cible) :
- couvrent tous les risques,
- couvrent les règles de sécurité (et les exigences réglementaires),
- sont pertinents vis-à-vis des hypothèses (et les enjeux du système-cible et le mode d'exploitation de sécurité).

La couleur orangée indique les éléments incomplètement couverts.

**Couverture des risques par les objectifs de sécurité**

| R.DISPO-ORGA | |
|---|---|
| Couverture | O.ORG-MOY<br>O.ORG-TRAV<br>O.PER-NORME<br>O.PER-POL<br>O.PER-VOLANT |
| Niveau de couverture | Couverture complète |
| Justification | Les 5 objectifs couvrent les vulnérabilités exploitées dans le risque ;<br>- Absence de plan de sensibilisation et de formation des processus de continuité des activités professionnelles<br>- Absence de processus de gestion de la continuité des activités professionnelles de l'organisme<br>- Absence de procédures de transfert de connaissances<br>- Présence d'épidémie virale locale |

| R.DISPO-PER | |
|---|---|
| Couverture | O.PER-ADHES<br>O.PER-POL<br>O.PER-VOLANT |
| Niveau de couverture | Couverture complète |
| Justification | Les 3 objectifs de sécurité couvrent l'ensemble des vulnérabilités exploitées dans le risque :<br>- Absence de procédures de transfert de connaissances<br>- Absentéisme<br>- Enieu concurrentiel |

| | |
|---|---|
| | - Maladie |

| R.DISPO-SUP | |
|---|---|
| Couverture | O.ORG-ARCHIV |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif de sécurité couvre la vulnérabilité exploitée dans le risque :<br>- Absence de procédure d'archivage des données contenues sur des supports (papier, magnétique) |

| R.DIV-LOG | |
|---|---|
| Couverture | O.LOG-AUTH |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Absence de vérification des accès partagés accordés au niveau logiciel |

| R.DIV-MAT | |
|---|---|
| Couverture | O.LOG-AUTH<br>O.MAT-ERG |
| Niveau de couverture | Couverture complète |
| Justification | Les 2 objectifs couvrent la vulnérabilité exploitée dans le risque :<br>- Absence de vérification des accès partagés accordés<br>- Fonctions de gestion des droits d'accès trop compliquées à utiliser et pouvant être source d'erreur<br>- Présence de répertoires partagés pour stocker de l'information. |

| R.DIV-ORGA | |
|---|---|
| Couverture | O.ORG-CONF<br>O.ORG-EXIG<br>O.ORG-POL-SYS<br>O.ORG-POL-SYS-SENS<br>O.ORG-ROLES |
| Niveau de couverture | Couverture complète |
| Justification | Les 5 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence d'identification des biens sensibles<br>- Absence d'organisation responsable de la définition, de la mise en oeuvre et du contrôle des privilèges d'accès à l'information<br>- Absence de contrôle des biens sensibles<br>- Absence de politique de protection de l'information<br>- La politique de sécurité n'est pas appliquée<br>- Les responsables sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous |

| R.DIV-PER | |
|---|---|
| Couverture | O.PER-IMP<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | Les 2 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence de sensibilisation à la protection de l'information à caractère sensible<br>- Absence de soutien de la direction à l'application de la politique de sécurité vis-à-vis du personne<br>- Non-respect des règles de classification de l'information |

| R.DIV-PHY | |
|---|---|
| Couverture | O.PHY-NORME |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Absence de contrôle des échanges avec l'extérieur |

| R.DIV-SUP | |
|---|---|
| Couverture | O.MAT-DIV |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Utilisation de supports capables d'effectuer des échanges d'information à caractère sensible (papier, clé USB, disquette...) |

| R.ECOUTE-LOG | |
|---|---|
| Couverture | O.LOG-AUTH<br>O.LOG-HABIL<br>O.ORG-CONF<br>O.ORG-PREUV |
| Niveau de couverture | Couverture complète |
| Justification | Les 4 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence de dispositif de contrôle accès en cas d'inactivité<br>- Absence de protection des journaux récoltant la trace des activités<br>- Absence de protection contre l'usage de privilèges avancés<br>- Pas de changement de mot de passe d'accès<br>- Possibilité d'ajout d'un logiciel d'écoute de type cheval de Troie |

| R.ECOUTE-ORGA | |
|---|---|
| Couverture | O.ORG-CONF<br>O.ORG-CONT-OBJ<br>O.ORG-EXIG<br>O.ORG-POL-SYS<br>O.ORG-ROLES |
| Niveau de couverture | Couverture complète |
| Justification | Les 5 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence d'identification des biens sensibles<br>- Absence de contrôle de l'application de la politique de sécurité<br>- La politique de sécurité n'est pas appliquée<br>- Les responsabilités de sécurité concernant la gestion des habilitations ne sont pas formalisées |

| R.ECOUTE-PER | |
|---|---|
| Couverture | O.PER-IMP<br>O.PER-SEC<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | Les 3 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Faible sensibilisation à la protection en confidentialité des échanges d'informations<br>- Absence de soutien de la direction à l'application de la politique de sécurité<br>- Manque de formation du personnel aux mesures et outils de protection des |

| | |
|---|---|
| | échanges externe et interne |
| **R.ECOUTE-PHY** | |
| Couverture | O.RES-INT |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Absence de protection d'accès au modem ADSL et au central téléphonique |
| **R.ECOUTE-RES** | |
| Couverture | O.RES-TRANS |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Utilisation de médium (Téléphone, ADSL, câble Ethernet) permettant la pose de matériel d'écoute |
| **R.ECOUTE-SITE** | |
| Couverture | O.PHY-ACCES |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Absence de contrôle d'accès au site |
| **R.ICENDIE-MAT-FIXE** | |
| Couverture | O.MAT-REMP<br>O.PHY-INCEND |
| Niveau de couverture | Couverture complète |
| Justification | Les 2 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence de matériels fixes de remplacement<br>- Utilisation de matériaux inflammables. |
| **R.INCENDIE-LOG** | |
| Couverture | O.LOG-LICEN |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Unicité des exemplaires des contrats de licence des logiciels |
| **R.INCENDIE-ORGA** | |
| Couverture | O.ORG-CONSIGN<br>O.ORG-CRISE<br>O.ORG-MAINTIEN<br>O.ORG-ROLES |
| Niveau de couverture | Couverture complète |
| Justification | Les 4 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence de procédures de sauvegarde des donnés contenues sur les supports<br>- Absence d'organisation de lutte contre l'incendie<br>- Absence d'affichage des informations à jour pour l'appel des services d'urgence |
| **R.INCENDIE-PER** | |
| Couverture | |

| | |
|---|---|
| | O.PER-INCID<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | Les 3 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence de test des procédures de réaction<br>- Absence d'information en cas de sinistre de la part du personnel. |

**R.INCENDIE-PHY**

| | |
|---|---|
| Couverture | O.PHY-INCEND<br>O.PHY-MAT-DANG |
| Niveau de couverture | Couverture complète |
| Justification | Les 2 objectifs couvrent la vulnérabilité exploitée dans le risque :<br>- Absence de prise en compte des risques d'incendie dans la phase d'installation du central téléphonique et du réseau électrique. |

**R.INCENDIE-SITE**

| | |
|---|---|
| Couverture | O.PHY-ACCES<br>O.PHY-INCEND |
| Niveau de couverture | Couverture complète |
| Justification | Les 2 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence de cloisonnement anti-feu<br>- Absence de contrôle d'accès au sein du site<br>- Présence d'ouverture sur la voie publique |

**R.INCENDIE-SUPPORT**

| | |
|---|---|
| Couverture | O.ORG-SAUV |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Absence de sauvegarde des données contenues sur le matériel transportable. |

**R.PIEGE-LOG**

| | |
|---|---|
| Couverture | O.LOG-CONF-SYS<br>O.LOG-HABIL |
| Niveau de couverture | Couverture complète |
| Justification | Les 2 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence de protection contre l'usage de privilèges avancés<br>- Absence de mise en oeuvre de règles de sécurité de base applicables au système d'exploitation et aux logiciels. |

**R.PIEGE-MAT**

| | |
|---|---|
| Couverture | O.MAT-AMOR |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Présence de matériel amorçable à partir d'un périphérique |

| R.PIEGE-ORGA | |
|---|---|
| Couverture | O.ORG-CONF<br>O.ORG-CONT-OBJ<br>O.ORG-POL-SYS<br>O.ORG-POL-SYS-SENS<br>O.ORG-PREUV<br>O.ORG-VIRUS |
| Niveau de couverture | Couverture complète |
| Justification | Les 6 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence d'identification des biens sensibles<br>- Absence de contrôle des biens sensibles<br>- Absence de conservation et d'analyse des traces des activités<br>- Absence de politique de protection des postes de travail<br>- Absence de politique globale de lutte contre le code malveillant |

| R.PIEGE-PER | |
|---|---|
| Couverture | O.PER-INCID<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | Les 2 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Manque de sensibilisation à la menace des codes malveillants<br>- Méconnaissance des procédures d'intervention et de réactions réflexes en cas de détection d'anomalie ou au non-respect des règles de mises à jour des logiciels anti-virus, vis-à-vis du personnel. |

| R.PIEGE-SUP | |
|---|---|
| Couverture | O.ORG-VIRUS |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif de sécurité couvre la vulnérabilité exploitée dans le risque :<br>- Absence de moyens permettant le contrôle d'innocuité des supports magnétiques (clé USB, disquette) lors de leurs entrées dans l'organisme |

| R.TELECOM-ORGA | |
|---|---|
| Couverture | O.ORG-CRISE |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Absence de maintenance des terminaux téléphoniques et Internet de la part de l'organisation |

| R.TELECOM-PER | |
|---|---|
| Couverture | O.PER-INCID<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | Les 2 objectifs couvrent la vulnérabilité exploitée dans le risque :<br>- Méconnaissance du personnel concernant les mesures de sécurité |

| R.TELECOM-PHY | |
|---|---|
| Couverture | O.PHY-SERVICES |
| Niveau de | Couverture partielle |

| | |
|---|---|
| couverture | |
| Justification | L'objectif couvre les vulnérabilités exploitées dans le risque :<br>- Dysfonctionnement des réseaux externes<br>- Défaut d'exploitation du réseau téléphonique interne<br>- Accès physique des locaux hébergeant les moyens de télécommunication non protégé<br>- Absence de la maintenance des équipements de télécommunication<br>- Absence de clauses contractuelles traitant du délai d'arrêt maximum admis pour la fourniture d'un service d'accès à Internet ou téléphonique<br><br>Il n'est toutefois pas possible de contrôler l'ensemble des fournitures de services essentiels. |
| **R.VOL-DOC-MAT** | |
| Couverture | O.MAT-DESCR<br>O.MAT-PROT |
| Niveau de couverture | Couverture complète |
| Justification | Les 2 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence d'inventaire du matériel<br>- Disques durs facilement démontables<br>- Présence de matériels attractifs. |
| **R.VOL-DOC-ORGA** | |
| Couverture | O.ORG-CONF<br>O.ORG-CONT-OBJ<br>O.ORG-EXIG<br>O.ORG-POL-SYS<br>O.ORG-POL-SYS-SENS<br>O.ORG-ROLES<br>O.ORG-SUIV-INCID |
| Niveau de couverture | Couverture complète |
| Justification | Les 7 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence d'identification des biens sensibles<br>- Absence d'organisation de gestion des incidents de sécurité<br>- Absence de contrôle de l'application de la politique de sécurité<br>- Absence de contrôle des biens sensibles<br>- La politique de sécurité n'est pas appliquée<br>- Les responsabilités de sécurité concernant la classification des informations ne sont pas formalisées ni connues de tous |
| **R.VOL-DOC-PER** | |
| Couverture | O.PER-SENSIB<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | Les 2 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence de sensibilisation à la protection des documents à caractère confidentiel<br>- Non respect des règles associées à la classification des informations de la part du personnel. |
| **R.VOL-DOC-SITE** | |
| Couverture | O.PHY-ACCES |
| Niveau de couverture | Couverture complète |

| | |
|---|---|
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Absence de contrôle d'accès au site |

**R.VOL-DOC-SUPPORT**

| | |
|---|---|
| Couverture | O.MAT-DESCR<br>O.MAT-PROT<br>O.MAT-RESTAU<br>O.ORG-CONF<br>O.ORG-SAUV<br>O.ORG-TRANS |
| Niveau de couverture | Couverture complète |
| Justification | Les 6 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence d'inventaire<br>- Absence de protection des supports<br>- Utilisation de supports accessibles par tous et aisément transportables<br>- Utilisation de supports originaux non sauvegardés |

**R.VOL-MAT-MAT**

| | |
|---|---|
| Couverture | O.MAT-DESCR<br>O.MAT-PROT<br>O.MAT-REMP |
| Niveau de couverture | Couverture complète |
| Justification | Les 3 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence de matériel de remplacement<br>- Absence d'inventaire<br>- Utilisation de matériel attractif, démontable |

**R.VOL-MAT-ORGA**

| | |
|---|---|
| Couverture | O.ORG-CONT-OBJ<br>O.ORG-POL-SYS<br>O.ORG-SUIV-INCID<br>O.ORG-VOL |
| Niveau de couverture | Couverture complète |
| Justification | Les 4 objectifs couvrent les vulnérabilités exploitées dans le risque :<br>- Absence d'identification des biens sensibles<br>- Absence d'organisation de gestion des incidents de sécurité lié au vol<br>- Absence de contrôle de l'application de la politique de sécurité et des entrées/sorties des matériels |

**R.VOL-MAT-PER**

| | |
|---|---|
| Couverture | O.PER-IMP<br>O.PER-RESP<br>O.PER-VOL |
| Niveau de couverture | Couverture complète |
| Justification | Les 3 objectifs couvrent la vulnérabilité exploitée dans le risque :<br>- Absence de soutien de la direction à l'application de la politique de sécurité<br>- Faible sensibilisation à la protection des matériels en dehors de l'organisme<br>- Non-respect des règles de protection des équipements transportables |

**R.VOL-MAT-SITE**

| | |
|---|---|
| Couverture | O.PHY-ACCES |

| | |
|---|---|
| Niveau de couverture | Couverture complète |
| Justification | L'objectif couvre la vulnérabilité exploitée dans le risque :<br>- Absence de contrôle d'accès au site |

**Couverture des enjeux par les objectifs de sécurité**

| H.REORGANISATION | |
|---|---|
| Couverture | O.ORG-MAINTIEN<br>O.ORG-PSSI<br>O.ORG-SAUV |
| Niveau de couverture | Couverture complète |
| Justification | Le système-cible étant au cœur des priorités du cabinet d'études, la continuité de ses activités est traitée par les objectifs de sécurité dans le respect de la PSSI. |

| H.INFORMATIQUE | |
|---|---|
| Couverture | O.ORG-CONSIGN<br>O.ORG-CRISE<br>O.ORG-MAINTIEN<br>O.ORG-ROLES |
| Niveau de couverture | Couverture complète |
| Justification | La cohérence des réflexions sur l'organisation du travail et des services avec celles sur l'informatique est assurée par des objectifs de sécurité d'organisation globale. |

| H.SERVICES | |
|---|---|
| Couverture | O.ORG-REGLEMENT<br>O.ORG-SSTRAIT<br>O.PER-VOLANT<br>O.PHY-SERVICES<br>O.RES-TRANS |
| Niveau de couverture | Couverture complète |
| Justification | Les services rendus et la qualité des prestations sont améliorés par la diminution des dysfonctionnements dans les échanges de données, la garantie de leur l'intégrité, la disponibilité de personnels et le respect de la réglementation en vigueur. |

| H.ECHANGES | |
|---|---|
| Couverture | O.MAT-AUTH-DOC<br>O.ORG-PSSI<br>O.ORG-SSTRAIT<br>O.RES-TRANS |
| Niveau de couverture | Couverture complète |
| Justification | Les échanges avec les autres organismes sont améliorés par la diminution des dysfonctionnements et la garantie de leur l'intégrité.<br>Les règles de la PSSI favoriseront la qualité des échanges avec les tiers. |

| H.METIERS | |
|---|---|
| Couverture | |

| | |
|---|---|
| | O.ORG-ROLES<br>O.PER-POL |
| Niveau de couverture | Couverture complète |
| Justification | La contribution aux évolutions des structures et des métiers est prise en compte dans une vision globale de la SSI fournie par une PSSI, son application par les personnels et la définition claire des rôles et responsabilités SSI. |

**Couverture des contraintes par les objectifs de sécurité**

| C.CONCURRENCE | |
|---|---|
| Couverture | O.ORG-PSSI |
| Niveau de couverture | Couverture complète |
| Justification | Dans un contexte de rude concurrence, la rapidité est essentielle. D'autre part, un important contrat avec une société est conditionné par la capacité du cabinet à assurer la confidentialité relative aux aspects techniques du projet.<br><br>L'élaboration d'une PSSI sur la base d'une analyse des risques SSI permet de garantir un système informatique sécurisé. |

| C.APPELS-OFFRES | |
|---|---|
| Couverture | O.RES-TRANS |
| Niveau de couverture | Couverture complète |
| Justification | Le cabinet d'études concourt pour de grands projets nationaux ou internationaux ; il s'appuie pour cela sur son système informatique qui lui permet de réagir extrêmement rapidement aux appels d'offre ou aux demandes des clients. L'entreprise doit maintenant répondre au souhait de la majorité des clients qui est de correspondre directement avec le bureau d'étude via Internet pour transmettre tous les types de documents (dossiers techniques, devis, appel d'offre, messages...).<br><br>Les 2 objectifs permettent de garantir un système informatique sécurisé. |

| C.CRISE | |
|---|---|
| Couverture | O.ORG-CRISE<br>O.PHY-INCEND<br>O.PHY-MAT-DANG<br>O.PHY-NORME<br>O.PHY-SERVICES |
| Niveau de couverture | Couverture complète |
| Justification | Seule une crise très grave dans le bâtiment pourrait affecter le fonctionnement du cabinet d'études.<br><br>L'organisation doit garantir une réaction rapide et efficace en cas de crise assurant une réduction des impacts potentiels et la continuité des activités essentielles : panne, sinistre, intrusion majeure, autre malveillance.<br><br>Une crise est couverte par les 6 objectifs de sécurité. |

| C.UTILISATEUR | |
|---|---|
| Couverture | O.ORG-PSSI |

| | |
|---|---|
| Niveau de couverture | Couverture complète |
| Justification | L'objectif tient compte de la contrainte. |

| C.RESPONSABLE | |
|---|---|
| Couverture | O.ORG-ROLES |
| Niveau de couverture | Couverture complète |
| Justification | Les objectifs de sécurité prennent en compte la contrainte. |

| C.NETTOYAGE | |
|---|---|
| Couverture | O.MAT-PROT<br>O.ORG-CONF<br>O.ORG-CONSIGN<br>O.ORG-VOL |
| Niveau de couverture | Couverture complète |
| Justification | Les objectifs de sécurité prennent en compte la contrainte. |

| C.CLIENTS | |
|---|---|
| Couverture | O.PHY-ACCES |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif de sécurité prend en compte cette contrainte |

| C.POINTE | |
|---|---|
| Couverture | O.ORG-PSSI |
| Niveau de couverture | Couverture complète |
| Justification | La mise en oeuvre de la PSSI doit prendre en compte la contrainte. |

| C.INVESTISSEMENT | |
|---|---|
| Couverture | O.ORG-PSSI |
| Niveau de couverture | Couverture complète |
| Justification | La PSSI tient compte de l'optimisation des investissements. |

| C.ARCHITECTURE | |
|---|---|
| Couverture | O.ORG-REGLEMENT |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif prend en compte la contrainte |

| C.LOGICIELS | |
|---|---|
| Couverture | O.LOG-LICEN<br>O.ORG-PSSI |
| Niveau de couverture | Couverture complète |
| Justification | La PSSI considère les logiciels professionnels du domaine architectural.<br>Par ailleurs, les licences de ces logiciels sont gérées dans le cadre des objectifs de sécurité. |

| C.IMMEUBLE | |
|---|---|
| Couverture | |

| | |
|---|---|
| | O.PHY-NORME |
| Niveau de couverture | Couverture complète |
| Justification | La situation du cabinet d'études est prise en compte dans les objectifs de sécurité. |
| **C.COMMERCES** | |
| Couverture | O.ORG-PSSI<br>O.PHY-ACCES |
| Niveau de couverture | Couverture complète |
| Justification | La PSSI et le contrôle d'accès physique traitent des aspects de sécurité physique en prenant en compte la contrainte. |
| **C.DEMENAGEMENT** | |
| Couverture | O.ORG-PSSI |
| Niveau de couverture | Couverture complète |
| Justification | L'analyse de risques SSI menant à l'élaboration de la PSSI considère les locaux existants. |
| **C.CONFIDENTIALITE** | |
| Couverture | O.ORG-CONF<br>O.PER-SENSIB<br>O.RES-TRANS |
| Niveau de couverture | Couverture complète |
| Justification | Les objectifs de sécurité prennent en compte la contrainte. |

**Couverture des références réglementaires par les objectifs de sécurité**

| | |
|---|---|
| **P.CNIL** | |
| Couverture | O.ORG-REGLEMENT |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif de sécurité couvre la référence réglementaire concernée :<br>- Déclaration à la CNIL des fichiers contenant des informations nominatives. |
| **P.901** | |
| Couverture | O.ORG-REGLEMENT |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif de sécurité couvre la référence réglementaire concernée :<br>respect de la recommandation n° 901. |
| **P.DDE** | |
| Couverture | O.ORG-REGLEMENT |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif de sécurité couvre la référence réglementaire concernée :<br>- Respect des règlements DDE. |

| P.MARCHES | |
|---|---|
| Couverture | O.ORG-REGLEMENT |
| Niveau de couverture | Couverture complète |
| Justification | L'objectif de sécurité couvre la référence réglementaire concernée :<br>- Respect du code des marchés publics. |

**Couverture des hypothèses par les objectifs de sécurité**

| H.USAGE | |
|---|---|
| Couverture | O.ORG-CONSIGN<br>O.ORG-ROLES<br>O.ORG-SAUV<br>O.PER-ADHES<br>O.PER-SENSIB<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | Les objectifs de sécurité tiennent compte des valeurs et axes stratégiques exprimés par le Directeur. |

| H.LOI | |
|---|---|
| Couverture | O.MAT-AUTH-DOC<br>O.ORG-REGLEMENT<br>O.ORG-ROLES<br>O.PER-SENSIB<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | Les objectifs de sécurité prennent en compte l'hypothèse. |

| H.POLICE | |
|---|---|
| Couverture | O.ORG-PSSI |
| Niveau de couverture | Couverture complète |
| Justification | L'analyse des risques SSI et la PSSI tiennent compte de l'hypothèse. |

**Couverture du mode d'exploitation par les objectifs de sécurité**

| H.DOMINANT | |
|---|---|
| Couverture | O.LOG-AUTH<br>O.LOG-HABIL<br>O.MAT-AUTH-DOC<br>O.RES-INT<br>O.RES-TRANS |
| Niveau de couverture | Couverture complète |
| Justification | Les objectifs de sécurité prennent en compte le mode d'exploitation de sécurité. |

**Couverture des règles de sécurité par les objectifs de sécurité**

| P.ALARME | |
|---|---|
| Couverture | O.ORG-PSSI<br>O.PHY-ACCES |
| Niveau de couverture | Couverture complète |
| Justification | L'activation d'une alarme durant les heures de fermeture concoure à la réduction de la facilité de pénétrer dans les locaux du cabinet d'études. |

| P.ARMOIRE-DISQ | |
|---|---|
| Couverture | O.ORG-CONSIGN<br>O.ORG-PSSI<br>O.ORG-ROLES<br>O.ORG-SAUV<br>O.PER-ADHES<br>O.PER-SENSIB<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | La PSSI comprend les règles relatives au stockage des sauvegardes et les autres objectifs de sécurité améliorent la responsabilisation des personnels. |

| P.ARMOIRE-DOC | |
|---|---|
| Couverture | O.ORG-CONSIGN<br>O.ORG-PSSI<br>O.ORG-ROLES<br>O.ORG-SAUV<br>O.PER-ADHES<br>O.PER-SENSIB<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | La PSSI comprend les règles relatives au stockage des documents papier et les autres objectifs de sécurité améliorent la responsabilisation des personnels. |

| P.INCENDIE | |
|---|---|
| Couverture | O.ORG-CONSIGN<br>O.ORG-CRISE<br>O.ORG-MAINTIEN<br>O.ORG-ROLES<br>O.ORG-SAUV |
| Niveau de couverture | Couverture complète |
| Justification | Les consignes, l'organisation et les mesures sécurité incendie cohérentes avec le système informatique sont compatibles avec les moyens réglementaires de lutte contre l'incendie. |

| P.INCENDIE-PLAN | |
|---|---|
| Couverture | O.ORG-CONSIGN<br>O.ORG-CRISE<br>O.ORG-MAINTIEN<br>O.ORG-ROLES<br>O.ORG-SAUV |
| Niveau de couverture | Couverture complète |

| | |
|---|---|
| Justification | Les consignes et l'organisation sécurité incendie traitent du plan de sécurité incendie qui sera cohérent avec le système informatique. |

**P.RESP-FICHIER**

| | |
|---|---|
| Couverture | O.MAT-AUTH-DOC<br>O.ORG-CONSIGN<br>O.ORG-PSSI<br>O.ORG-ROLES<br>O.ORG-SAUV<br>O.PER-ADHES<br>O.PER-SENSIB<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | La PSSI comprend les règles relatives aux responsabilités des personnels, les objectifs de sécurité suivants améliorent la responsabilisation des personnels et le dernier leur offre un moyen de protéger les fichiers dont ils sont responsables. |

**P.SAUVEGARDE**

| | |
|---|---|
| Couverture | O.ORG-CONSIGN<br>O.ORG-PSSI<br>O.ORG-ROLES<br>O.ORG-SAUV<br>O.PER-ADHES<br>O.PER-SENSIB<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | La PSSI comprend les règles relatives à la sauvegarde de tout fichier et les autres objectifs de sécurité améliorent la responsabilisation des personnels. |

**P.CONTROLE-ACCES**

| | |
|---|---|
| Couverture | O.ORG-PSSI |
| Niveau de couverture | Couverture complète |
| Justification | La PSSI comprend les règles relatives au contrôle d'accès des utilisateurs, celui-ci pouvant s'effectuer par identifiant / mot de passe. |

**P.FERMETURE**

| | |
|---|---|
| Couverture | O.ORG-CONSIGN<br>O.ORG-ROLES<br>O.ORG-SAUV<br>O.PER-ADHES<br>O.PER-SENSIB<br>O.PER-USAGE |
| Niveau de couverture | Couverture complète |
| Justification | La fermeture à clé des locaux contribue à la réduction de la facilité de pénétrer dans les locaux, tout comme les objectifs de sécurité améliorant la responsabilisation des personnels du cabinet d'études. |

### 6.2.3 Justification des objectifs de sécurité

Les tableaux-croisés ci-dessous démontrent que chaque objectif de sécurité répond au moins à un risque, une règle de politique de sécurité (ou une exigence réglementaire) ou une hypothèse (ou un enjeu du système-cible ou au mode d'exploitation de sécurité).
La couleur orangée indique les éléments incomplètement couverts.

1ère partie des objectifs de sécurité :

| | O.LOG-AUTH | O.LOG-CONF-SYS | O.LOG-HABIL | O.LOG-LICEN | O.MAT-AMOR | O.MAT-AUTH-DOC | O.MAT-DESCR | O.MAT-DIV | O.MAT-ERG | O.MAT-PROT | O.MAT-REMP | O.MAT-RESTAU | O.ORG-ARCHIV | O.ORG-CONF | O.ORG-CONSIGN | O.ORG-CONT-OBJ | O.ORG-CRISE | O.ORG-EQMT | O.ORG-EXIG | O.ORG-MAINTIEN | O.ORG-MOY | O.ORG-POL-SYS | O.ORG-POL-SYS-SENS | O.ORG-PREUV | O.ORG-PSSI | O.ORG-REGLEMENT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R.DISPO-ORGA | | | | | | | | | | | | | | | | | | | | | X | | | | | |
| R.DISPO-PER | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.DISPO-SUP | | | | | | | | | | | | | X | | | | | | | | | | | | | |
| R.DIV-LOG | X | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.DIV-MAT | X | | | | | | | | X | | | | | | | | | | | | | | | | | |
| R.DIV-ORGA | | | | | | | | | | | | | | X | | | | | X | | | X | X | | | |
| R.DIV-PER | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.DIV-PHY | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.DIV-SUP | | | | | | | | X | | | | | | | | | | | | | | | | | | |
| R.ECOUTE-LOG | X | | X | | | | | | | | | | | X | | | | | | | | | | X | | |
| R.ECOUTE-ORGA | | | | | | | | | | | | | | X | | X | | | X | | | X | | | | |
| R.ECOUTE-PER | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.ECOUTE-PHY | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.ECOUTE-RES | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.ECOUTE-SITE | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.ICENDIE-MAT-FIXE | | | | | | | | | | | X | | | | | | | | | | | | | | | |
| R.INCENDIE-LOG | | | | X | | | | | | | | | | | | | | | | | | | | | | |
| R.INCENDIE-ORGA | | | | | | | | | | | | | | | X | | X | | | X | | | | | | |
| R.INCENDIE-PER | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.INCENDIE-PHY | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.INCENDIE-SITE | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.INCENDIE-SUPPORT | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.PIEGE-LOG | | X | X | | | | | | | | | | | | | | | | | | | | | | | |
| R.PIEGE-MAT | | | | | X | | | | | | | | | | | | | | | | | | | | | |
| R.PIEGE-ORGA | | | | | | | | | | | | | | X | | X | | | | | | X | X | X | | |
| R.PIEGE-PER | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.PIEGE-SUP | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.TELECOM-ORGA | | | | | | | | | | | | | | | | | X | | | | | | | | | |
| R.TELECOM-PER | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.TELECOM-PHY | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.VOL-DOC-MAT | | | | | | | X | | | X | | | | | | | | | | | | | | | | |
| R.VOL-DOC-ORGA | | | | | | | | | | | | | | X | | X | | | X | | | X | X | | | |
| R.VOL-DOC-PER | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | O.LOG-AUTH | O.LOG-CONF-SYS | O.LOG-HABIL | O.LOG-LICEN | O.MAT-AMOR | O.MAT-AUTH-DOC | O.MAT-DESCR | O.MAT-DIV | O.MAT-ERG | O.MAT-PROT | O.MAT-REMP | O.MAT-RESTAU | O.ORG-ARCHIV | O.ORG-CONF | O.ORG-CONSIGN | O.ORG-CONT-OBJ | O.ORG-CRISE | O.ORG-EQMT | O.ORG-EXIG | O.ORG-MAINTIEN | O.ORG-MOY | O.ORG-POL-SYS | O.ORG-POL-SYS-SENS | O.ORG-PREUV | O.ORG-PSSI | O.ORG-REGLEMENT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R.VOL-DOC-SITE | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.VOL-DOC-SUPPORT | | | | | | | X | | | X | | X | | X | | | | | | | | | | | | |
| R.VOL-MAT-MAT | | | | | | | X | | | X | X | | | | | | | | | | | | | | | |
| R.VOL-MAT-ORGA | | | | | | | | | | | | | | | | X | | | | | | X | | | | |
| R.VOL-MAT-PER | | | | | | | | | | | | | | | | | | | | | | | | | | |
| R.VOL-MAT-SITE | | | | | | | | | | | | | | | | | | | | | | | | | | |
| H.ECHANGES | | | | | | X | | | | | | | | | | | | | | | | | | | X | |
| H.INFORMATIQUE | | | | | | | | | | | | | | | X | | X | | | X | | | | | | |
| H.METIERS | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| H.REORGANISATION | | | | | | | | | | | | | | | | | | | | X | | | | | X | |
| H.SERVICES | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| C.APPELS-OFFRES | | | | | | | | | | | | | | | | | | | | | | | | | | |
| C.ARCHITECTURE | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| C.CLIENTS | | | | | | | | | | | | | | | | | | | | | | | | | | |
| C.CLIMATISATION | | | | | | | | | | | | | | | | | | X | | | | | | | | |
| C.COMMERCES | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| C.CONCURRENCE | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| C.CONFIDENTIALITE | | | | | | | | | | | | | | X | | | | | | | | | | | | |
| C.CRISE | | | | | | | | | | | | | | | | | X | | | | | | | | | |
| C.DEMENAGEMENT | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| C.IMMEUBLE | | | | | | | | | | | | | | | | | | | | | | | | | | |
| C.INVESTISSEMENT | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| C.LOGICIELS | | | | X | | | | | | | | | | | | | | | | | | | | | X | |
| C.NETTOYAGE | | | | | | | | | | X | | | | X | X | | | | | | | | | | | |
| C.POINTE | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| C.RESPONSABLE | | | | | | | | | | | | | | | | | | | | | | | | | | |
| C.UTILISATEUR | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| P.901 | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| P.CNIL | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| P.DDE | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| P.MARCHES | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| H.LOI | | | | | | X | | | | | | | | | | | | | | | | | | | | X |
| H.POLICE | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| H.USAGE | | | | | | | | | | | | | | | X | | | | | | | | | | | |
| H.DOMINANT | X | | X | | | X | | | | | | | | | | | | | | | | | | | | |
| P.ALARME | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| P.ARMOIRE-DISQ | | | | | | | | | | | | | | | X | | | | | | | | | | X | |
| P.ARMOIRE-DOC | | | | | | | | | | | | | | | X | | | | | | | | | | X | |
| P.CONTROLE-ACCES | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| P.FERMETURE | | | | | | | | | | | | | | | X | | | | | | | | | | | |
| P.INCENDIE | | | | | | | | | | | | | | | X | | X | | | X | | | | | | |

| | O.LOG-AUTH | O.LOG-CONF-SYS | O.LOG-HABIL | O.LOG-LICEN | O.MAT-AMOR | O.MAT-AUTH-DOC | O.MAT-DESCR | O.MAT-DIV | O.MAT-ERG | O.MAT-PROT | O.MAT-REMP | O.MAT-RESTAU | O.ORG-ARCHIV | O.ORG-CONF | O.ORG-CONSIGN | O.ORG-CONT-OBJ | O.ORG-CRISE | O.ORG-EQMT | O.ORG-EXIG | O.ORG-MAINTIEN | O.ORG-MOY | O.ORG-POL-SYS | O.ORG-POL-SYS-SENS | O.ORG-PREUV | O.ORG-PSSI | O.ORG-REGLEMENT |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P.INCENDIE-PLAN | | | | | | | | | | | | | | | X | | X | | | X | | | | | | |
| P.RESP-FICHIER | | | | | | X | | | | | | | | | X | | | | | | | | | | X | |
| P.SAUVEGARDE | | | | | | | | | | | | | | | X | | | | | | | | | | X | |

2nde partie des objectifs de sécurité :

| | O.ORG-ROLES | O.ORG-SAUV | O.ORG-SSTRAIT | O.ORG-SUIV-INCID | O.ORG-TRANS | O.ORG-TRAV | O.ORG-VIRUS | O.ORG-VOL | O.PER-ADHES | O.PER-IMP | O.PER-INCID | O.PER-NORME | O.PER-POL | O.PER-RESP | O.PER-SEC | O.PER-SENSIB | O.PER-USAGE | O.PER-VOL | O.PER-VOLANT | O.PHY-ACCES | O.PHY-INCEND | O.PHY-MAT-DANG | O.PHY-NORME | O.RES-INT | O.PHY-SERVICES | O.RES-TRANS | **Couverture** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R.DISPO-ORGA | | | | | | X | | | | | | X | X | | | | | | X | | | | | | | | **2** |
| R.DISPO-PER | | | | | | | | | X | | | | X | | | | | | X | | | | | | | | **2** |
| R.DISPO-SUP | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.DIV-LOG | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.DIV-MAT | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.DIV-ORGA | X | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.DIV-PER | | | | | | | | | | X | | | | | | | X | | | | | | | | | | **2** |
| R.DIV-PHY | | | | | | | | | | | | | | | | | | | | | | | X | | | | **2** |
| R.DIV-SUP | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.ECOUTE-LOG | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.ECOUTE-ORGA | X | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.ECOUTE-PER | | | | | | | | | | X | | | | | X | | X | | | | | | | | | | **2** |
| R.ECOUTE-PHY | | | | | | | | | | | | | | | | | | | | | | | | X | | | **2** |
| R.ECOUTE-RES | | | | | | | | | | | | | | | | | | | | | | | | | | X | **2** |
| R.ECOUTE-SITE | | | | | | | | | | | | | | | | | | | | X | | | | | | | **2** |
| R.ICENDIE-MAT-FIXE | | | | | | | | | | | | | | | | | | | | | X | | | | | | **2** |
| R.INCENDIE-LOG | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.INCENDIE-ORGA | X | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.INCENDIE-PER | | | | | | | | | X | | X | | | | | | X | | | | | | | | | | **2** |
| R.INCENDIE-PHY | | | | | | | | | | | | | | | | | | | | | X | X | | | | | **2** |
| R.INCENDIE-SITE | | | | | | | | | | | | | | | | | | | | X | X | | | | | | **2** |
| R.INCENDIE-SUPPORT | | X | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.PIEGE-LOG | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.PIEGE-MAT | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.PIEGE-ORGA | | | | | | | X | | | | | | | | | | | | | | | | | | | | **2** |
| R.PIEGE-PER | | | | | | | | | | | X | | | | | | X | | | | | | | | | | **2** |
| R.PIEGE-SUP | | | | | | | X | | | | | | | | | | | | | | | | | | | | **2** |

| | O.ORG-ROLES | O.ORG-SAUV | O.ORG-SSTRAIT | O.ORG-SUIV-INCID | O.ORG-TRANS | O.ORG-TRAV | O.ORG-VIRUS | O.ORG-VOL | O.PER-ADHES | O.PER-IMP | O.PER-INCID | O.PER-NORME | O.PER-POL | O.PER-RESP | O.PER-SEC | O.PER-SENSIB | O.PER-USAGE | O.PER-VOL | O.PER-VOLANT | O.PHY-ACCES | O.PHY-INCEND | O.PHY-MAT-DANG | O.PHY-NORME | O.RES-INT | O.PHY-SERVICES | O.RES-TRANS | **Couverture** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R.TELECOM-ORGA | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.TELECOM-PER | | | | | | | | | | | X | | | | | | X | | | | | | | | | | **2** |
| R.TELECOM-PHY | | | | | | | | | | | | | | | | | | | | | | | | | X | | **1** |
| R.VOL-DOC-MAT | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.VOL-DOC-ORGA | X | | | X | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.VOL-DOC-PER | | | | | | | | | | | | | | | | X | X | | | | | | | | | | **2** |
| R.VOL-DOC-SITE | | | | | | | | | | | | | | | | | | | | X | | | | | | | **2** |
| R.VOL-DOC-SUPPORT | | X | | | X | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.VOL-MAT-MAT | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| R.VOL-MAT-ORGA | | | | X | | | | X | | | | | | | | | | | | | | | | | | | **2** |
| R.VOL-MAT-PER | | | | | | | | | | X | | | | X | | | | X | | | | | | | | | **2** |
| R.VOL-MAT-SITE | | | | | | | | | | | | | | | | | | | | X | | | | | | | **2** |
| H.ECHANGES | | | X | | | | | | | | | | | | | | | | | | | | | | | X | **2** |
| H.INFORMATIQUE | X | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| H.METIERS | X | | | | | | | | | | | | X | | | | | | | | | | | | | | **2** |
| H.REORGANISATION | | X | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| H.SERVICES | | | X | | | | | | | | | | | | | | | | X | | | | | | X | X | **2** |
| C.APPELS-OFFRES | | | | | | | | | | | | | | | | | | | | | | | | | | X | **2** |
| C.ARCHITECTURE | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| C.CLIENTS | | | | | | | | | | | | | | | | | | | | X | | | | | | | **2** |
| C.CLIMATISATION | | | | | | | | | | | | | | | | | | | | | | | | | X | | **2** |
| C.COMMERCES | | | | | | | | | | | | | | | | | | | | X | | | | | | | **2** |
| C.CONCURRENCE | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| C.CONFIDENTIALITE | | | | | | | | | | | | | | | | X | | | | | | | | | | X | **2** |
| C.CRISE | | | | | | | | | | | | | | | | | | | | | X | X | X | | X | | **2** |
| C.DEMENAGEMENT | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| C.IMMEUBLE | | | | | | | | | | | | | | | | | | | | | X | | X | | | | **2** |
| C.INVESTISSEMENT | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| C.LOGICIELS | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| C.NETTOYAGE | | | | | | | | X | | | | | | | | | | | | | | | | | | | **2** |
| C.POINTE | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| C.RESPONSABLE | X | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| C.UTILISATEUR | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| P.901 | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| P.CNIL | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| P.DDE | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| P.MARCHES | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| H.LOI | X | | | | | | | | | | | | | | | X | X | | | | | | | | | | **2** |
| H.POLICE | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| H.USAGE | X | X | | | | | | | X | | | | | | | X | X | | | | | | | | | | **2** |
| H.DOMINANT | | | | | | | | | | | | | | | | | | | | | | | | X | | X | **2** |
| P.ALARME | | | | | | | | | | | | | | | | | | | | X | | | | | | | **2** |

| | O.ORG-ROLES | O.ORG-SAUV | O.ORG-SSTRAIT | O.ORG-SUIV-INCID | O.ORG-TRANS | O.ORG-TRAV | O.ORG-VIRUS | O.ORG-VOL | O.PER-ADHES | O.PER-IMP | O.PER-INCID | O.PER-NORME | O.PER-POL | O.PER-RESP | O.PER-SEC | O.PER-SENSIB | O.PER-USAGE | O.PER-VOL | O.PER-VOLANT | O.PHY-ACCES | O.PHY-INCEND | O.PHY-MAT-DANG | O.PHY-NORME | O.RES-INT | O.PHY-SERVICES | O.RES-TRANS | **Couverture** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| P.ARMOIRE-DISQ | X | X | | | | | | | X | | | | | | | X | X | | | | | | | | | | **2** |
| P.ARMOIRE-DOC | X | X | | | | | | | X | | | | | | | X | X | | | | | | | | | | **2** |
| P.CONTROLE-ACCES | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| P.FERMETURE | X | X | | | | | | | X | | | | | | | X | X | | | | | | | | | | **2** |
| P.INCENDIE | X | X | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| P.INCENDIE-PLAN | X | X | | | | | | | | | | | | | | | | | | | | | | | | | **2** |
| P.RESP-FICHIER | X | X | | | | | | | X | | | | | | | X | X | | | | | | | | | | **2** |
| P.SAUVEGARDE | X | X | | | | | | | X | | | | | | | X | X | | | | | | | | | | **2** |

## 6.3 Activité 3 : Détermination des niveaux de sécurité

*Cette activité a pour but de choisir les niveaux de sécurité, en termes de :*
- *niveaux de résistance[1] des objectifs de sécurité,*
- *de niveau d'assurance[2].*

*Nous considérons trois niveaux de résistance pour les objectifs de sécurité :*

| | |
|---|---|
| *Niveau élémentaire* | *Un 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.* |
| *Niveau moyen* | *Un 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 œuvre ou une violation intentionnelle de la sécurité du système par des attaquants possédant un potentiel d'attaque modéré.* |
| *Niveau élevé* | *Un 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.* |

*Concernant les objectifs de sécurité couvrant des risques, le niveau requis dépend essentiellement du potentiel d'attaque (mais aussi des besoins de sécurité et de l'opportunité des menaces). Si un objectif de sécurité couvre plusieurs risques dont les potentiels d'attaque diffèrent, on retient le niveau le plus élevé.*
*Concernant les objectifs de sécurité couvrant les règles de sécurité (ou les exigences réglementaires), leur niveau est choisi par l'organisme en fonction de l'importance qu'il accorde à celles-ci et des efforts qu'il compte mettre en œuvre pour les faire respecter.*

*Quant aux niveaux d'assurance, il en existe 7 prédéfinis :*

| | |
|---|---|
| *Niveau 1* | *Testé fonctionnellement* |
| *Niveau 2* | *Testé structurellement* |
| *Niveau 3* | *Testé et vérifié méthodiquement* |
| *Niveau 4* | *Conçu, testé et revu méthodiquement* |
| *Niveau 5* | *Conçu à l'aide de méthode semi-formelles et testé* |
| *Niveau 6* | *Conception vérifiée à l'aide de méthodes semi-formelles et testé* |
| *Niveau 7* | *Conception vérifiée à l'aide de méthodes formelles et testé* |

*Ces niveaux sont composés de différents composants de rigueur croissante qui permettent d'évaluer la sécurité mise en œuvre.*

*Le niveau d'assurance représente le niveau de confiance que l'on peut accorder à la mise en œuvre des exigences fonctionnelles de sécurité. Plus il est élevé, plus l'organisme disposera de garanties sur*

[1] Niveaux issus de la définition des niveaux de résistance des fonctions de l'ISO/IEC 15408.
[2] Le niveau d'assurance représente un paquet de composants d'assurance tirés de la Partie 3 de l'ISO/IEC 15408 qui représente un niveau de l'échelle d'assurance prédéfinie.

*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.*

*Il est aussi possible pour l'organisme de définir ses propres exigences d'assurance en choisissant des exigences parmi les composants existants ou même d'en définir de nouveaux.*

### 6.3.1 Niveaux requis pour les objectifs de sécurité

Le tableau suivant présente les niveaux des objectifs de sécurité du cabinet d'études, avec leur niveau de résistance et des justifications :

| | Niveau de résistance | Justification |
|---|---|---|
| O.LOG-AUTH | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.LOG-CONF-SYS | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.LOG-HABIL | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.LOG-LICEN | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.MAT-AMOR | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.MAT-AUTH-DOC | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.MAT-DESCR | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.MAT-DIV | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.MAT-ERG | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.MAT-PROT | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.MAT-RESTAU | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.MAT-REMP | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-ACCES | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-ARCHIV | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une |

| | | |
|---|---|---|
| | | mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-CONF | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-CONSIGN | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-CONT-OBJ | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-CRISE | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-EQMT | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-EXIG | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-MAINTIEN | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-MOY | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-PASS | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-POL-SYS | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-POL-SYS-SENS | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-PREUV | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-PSSI | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-REGLEMENT | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-ROLES | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-SAUV | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-SSTRAIT | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-SUIV- | 2 | Décision du comité de pilotage sur la base des risques concernés |

| | | |
|---|---|---|
| INCID | | (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-TRANS | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-TRAV | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-VIRUS | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.ORG-VOL | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-ADHES | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-IMP | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-INCID | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-NORME | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-POL | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-RESP | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-SEC | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-SENSIB | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-USAGE | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-VOL | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PER-VOLANT | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PHY-ACCES | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PHY-INCEND | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |

| | | |
|---|---|---|
| O.PHY-MAT-DANG | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PHY-NORME | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.RES-INT | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.PHY-SERVICES | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| O.RES-TRANS | 2 | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |

### 6.3.2 Choix du niveau d'assurance

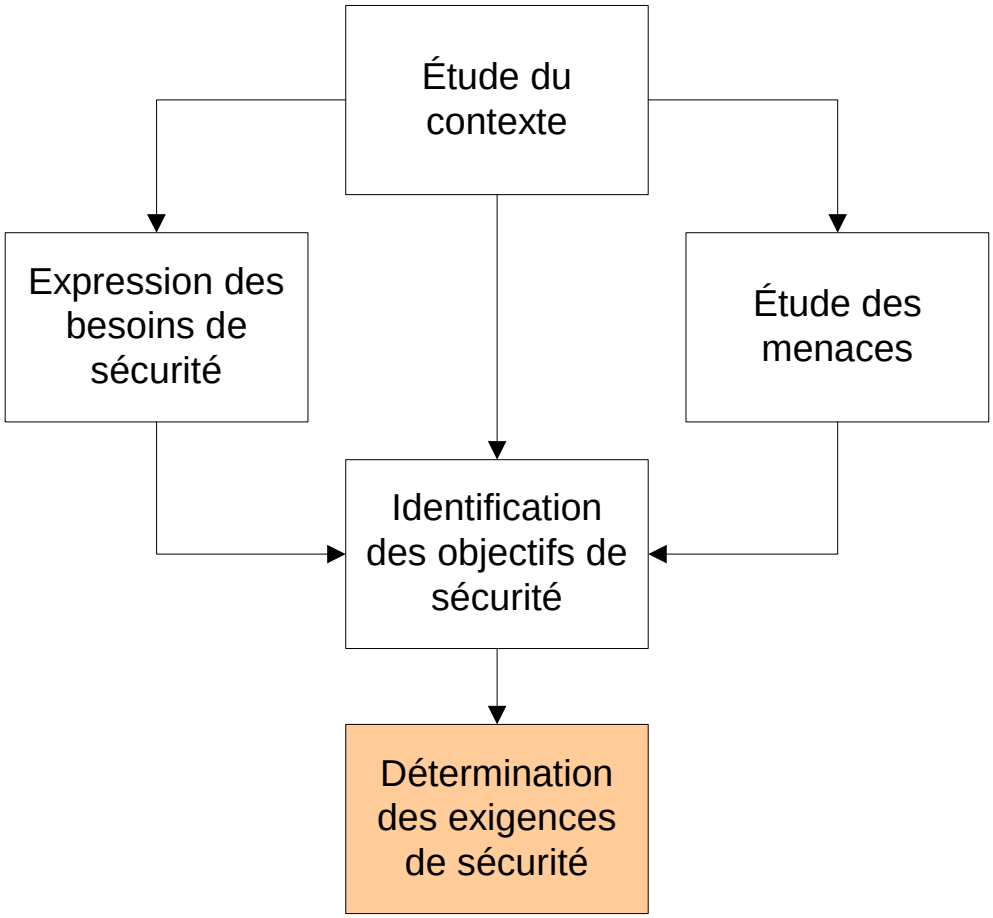
| **EAL1** | |
|---|---|
| Exigences d'assurance sélectionnées | ADV_FSP.1<br>ADO_IGS.1<br>ACM_CAP.1<br>ATE_IND.1<br>AGD_USR.1<br>AGD_ADM.1<br>ADV_RCR.1 |
| Justification | Pour son système d'information, le choix du cabinet d'études se porte sur un niveau d'assurance EAL 1 pour plusieurs raisons :<br><br>Paramètres :<br>- La taille et les capacités du cabinet d'études sont réduites<br>- Le système d'information existe déjà (ce n'est pas un système d'information à concevoir)<br>- Le cabinet d'études ne possède pas d'expérience pour définir de nouveaux composants<br>- Aucune information classifiée de défense n'est traitée par le système d'information<br>- Les risques sont gérés (appréciés, traités et communiqués) en utilisant une méthodologie (la présente étude)<br><br>Conséquences :<br>- Le niveau est limité en terme de coût<br>- Le cabinet d'études ne peut requérir de trop hautes exigences à ses fournisseurs<br>- Les exigences d'assurance sont limitées à celles qui existent déjà dans la Partie 3 de l'ISO/IEC 15408<br>- L'utilisation de matériels évalués et certifiés à un niveau d'assurance particulier n'est pas requise<br>- La confiance envers la SSI augmente largement dès lors que les risques sont gérés<br><br>Selon, l'ISO/IEC 15408, le niveau EAL 1 est applicable quand une certaine |

contre la sécurité ne sont pas considérées comme sérieuses. Ce niveau présentera un intérêt quand une assurance, obtenue de façon indépendante, est nécessaire pour confirmer qu'un soin approprié aura été apporté pour protéger les informations personnelles ou similaires.

Le niveau EAL 1 permet d'obtenir une évaluation du système, telle qu'elle est disponible à l'utilisateur, comprenant des tests indépendants par rapport à une spécification, ainsi qu'un examen des guides fournis. Une évaluation de niveau EAL 1 doit pouvoir être réalisée avec succès sans l'assistance du développeur du système et avec un coût minimal.

Une évaluation effectuée à ce niveau devrait procurer des éléments de preuve que le système fonctionne d'une manière conforme à celle décrite dans sa documentation et qu'elle fournit une protection utile contre les menaces identifiées.

# 7 Étape 5 : Détermination des exigences de sécurité



## 7.1 Activité 1 : Détermination des exigences de sécurité fonctionnelles

*La détermination des exigences de sécurité fonctionnelles s'effectue en fonction des objectifs de sécurité identifiés.*

*Ces exigences fonctionnelles peuvent être issues de l'ISO/IEC 15408 (critères communs) ou créées de toute pièce.*
*Les exigences de sécurité résultent du raffinement des objectifs de sécurité en un ensemble d'exigences de sécurité pour la cible de l'étude de sécurité et d'exigences de sécurité pour l'environnement qui, si elles sont satisfaites, garantiront que la cible de l'étude de sécurité peut satisfaire à ses objectifs de sécurité.*
*Les exigences fonctionnelles sont imposées aux fonctions de la cible de l'étude de sécurité qui supportent tout particulièrement la sécurité des technologies de l'information et qui déterminent le comportement voulu en terme de sécurité.*

*La détermination des exigences de sécurité fonctionnelles nécessite de prendre en compte tous les éléments du contexte, notamment les contraintes budgétaires et techniques. Cette activité requiert l'obtention d'un consensus sur les moyens qui permettront de réaliser les objectifs de sécurité. Ce consensus ne peut être obtenu qu'en comparant les risques encourus au coût des mesures de sécurité correspondant aux exigences de sécurité fonctionnelles envisagées.*

*Une matrice de couverture doit être réalisée afin de s'assurer que tous les objectifs de sécurité de la cible de l'étude de sécurité sont couverts par au moins une exigence de sécurité fonctionnelle.*

### 7.1.1 Formalisation des exigences de sécurité fonctionnelles

Les exigences de sécurité fonctionnelles pour le cabinet d'études devraient satisfaire ses objectifs de sécurité au niveau de résistance requis.

Il se peut néanmoins que la couverture soit incomplète du fait de la difficulté ou du coût de la mise en œuvre de ces exigences. C'est pourquoi les données de l'étude EBIOS sont nécessaires pour apprécier l'impact des risques par rapport aux moyens à mettre en œuvre.

Il convient alors de présenter la couverture des objectifs de sécurité par les exigences et de mettre en évidence les éventuels risques résiduels à l'issu de cette réflexion.

Pour le cabinet d'études, les exigences sont rédigées de toute pièce mais elles pourront être enrichies ultérieurement à l'aide d'exigences issues de l'ISO/IEC 15408 pour les parties techniques.

Voici une liste de 83 exigences de sécurité fonctionnelles déterminées pour le cabinet d'études et créées directement à la suite de l'analyse :

| **EF.LOG-ACCES** | |
|---|---|
| Description | Des mécanismes de contrôle d'accès aux ressources du cabinet d'études sont à mettre en oeuvre via les fonctionnalités du système d'exploitation. |
| **EF.LOG-ARCHIV-CONTR** | |
| Description | Les archives doivent être signées électroniquement et la signature doit être vérifiée périodiquement. |
| **EF.LOG-AUTH** | |
| Description | Le cabinet d'études doit mettre en oeuvre un mécanisme d'authentification forte pour l'accès au système sur la base de l'utilisation de certificats. |
| **EF.LOG-BESOINS** | |
| Description | |

| | |
|---|---|
| | les éléments du système d'information en fonction de leur besoin d'en connaître ou d'en modifier et non en fonction de leur position hiérarchique. |

**EF.LOG-CHIFFREMENT**

| | |
|---|---|
| Description | Le cabinet d'études doit disposer de mécanismes de chiffrement de données et de flux. |

**EF.LOG-CONFIG**

| | |
|---|---|
| Description | Les configurations matérielles (BIOS) et logicielles (système d'exploitation) ne doivent pas permettre le démarrage des postes à partir d'un périphérique amovible (clé USB, disquette, cédérom...). |

**EF.LOG-CONTR**

| | |
|---|---|
| Description | Le cabinet d'études doit mettre en place un contrôle périodique de la configuration des systèmes et applications afin de s'assurer de la conformité à la politique de sécurité. |

**EF.LOG-DOC**

| | |
|---|---|
| Description | L'ensemble des documents électroniques doit être pris en compte dans la politique de sauvegarde. |

**EF.LOG-FILTRE**

| | |
|---|---|
| Description | Les connexions doivent être filtrées de manière à ne pas permettre le trafic non prévu (exploitation de fonctionnement asynchrone, accès sur des ports non autorisés, spam...). |

**EF.LOG-MESSAGERIE**

| | |
|---|---|
| Description | La configuration de la messagerie électronique doit permettre de maîtriser les flux réseaux générés (réduction des émissions automatiques, listes de diffusion accessibles à tous...). |

**EF.LOG-ORIGINE**

| | |
|---|---|
| Description | L'origine des installations, matériels ou logiciels et de leurs mises à jour doit pouvoir être garantie. |

**EF.LOG-POSTES**

| | |
|---|---|
| Description | La politique de sécurité doit inclure une politique de protection des postes de travail fixes et nomades (intégrité, contrôle d'accès, lutte contre les codes malveillants...). |

**EF.LOG-PRIVIL**

| | |
|---|---|
| Description | L'attribution et l'utilisation de privilèges doivent être restreintes et maîtrisées. |

**EF.LOG-SAUV**

| | |
|---|---|
| Description | Des copies de sauvegarde des logiciels essentiels, des traces (journaux d'événements), des configurations des systèmes d'exploitation et des applications doivent être faites et testées à intervalles réguliers. |

**EF.LOG-SERVICES**

| | |
|---|---|
| Description | Les utilisateurs ne doivent pouvoir accéder directement qu'aux services spécifiques qu'ils ont été autorisés à utiliser. |

**EF.LOG-SIGNATURE**

| | |
|---|---|
| Description | Les personnels du cabinet d'études doivent pouvoir signer électroniquement leurs échanges et leurs documents à l'aide d'un certificat électronique. |

**EF.LOG-TRACES-DETEC**

| | |
|---|---|
| Description | Des règles doivent permettre d'analyser les événements audités pour détecter des violations potentielles de la sécurité. |

**EF.LOG-TRACES-EXPL**

| | |
|---|---|
| Description | Le cabinets d'études doit disposer d'outils d'exploitation des traces.<br>Les procédures d'exploitation du système d'information doivent y faire référence. |

**EF.LOG-TRACES-GEN**

| | |
|---|---|
| Description | Le système doit pouvoir générer un enregistrement d'audit des événements auditables suivants : [à définir]. |

**EF.LOG-TRACES-STOCK**

| | |
|---|---|
| Description | Les enregistrements d'audit stockés doivent être protégés contre une suppression non autorisée. |

**EF.LOG-USAGE**

| | |
|---|---|
| Description | Les logiciels utilisés doivent être communément employés ou avoir été audité. |

**EF.LOG-VIRUS-DETEC**

| | |
|---|---|
| Description | Des mesures de maîtrise de détection et de prévention doivent être mises en œuvre afin de fournir une protection contre les logiciels malveillants (deux antivirus mis à jour régulièrement) ainsi que des procédures appropriées de sensibilisation des utilisateurs doivent être mises en œuvre. |

**EF.MAT-ANTIVOL**

| | |
|---|---|
| Description | Des mesures techniques de type antivol doivent être mis en oeuvre pour protéger les matériels du cabinet d'études. |

**EF.MAT-BUREAU**

| | |
|---|---|
| Description | Les matériels et les supports doivent être rangés sous clé en cas d'absence prolongée du personnel du cabinet d'études. |

**EF.MAT-DIM**

| | |
|---|---|
| Description | L'ensemble des secours (redondant ou non) doit être dimensionné de manière à fournir une qualité de service correspondant aux objectifs identifiés pour les solutions dégradées de secours. |

**EF.MAT-EXT**

| | |
|---|---|
| Description | Des procédures et des mesures de maîtrise de sécurité doivent être utilisées afin de sécuriser le matériel utilisé à l'extérieur des locaux d'un organisme. |

**EF.MAT-INSTALL**

| | |
|---|---|
| Description | Les éventuels risques spécifiques aux éléments hébergés dans l'organisme (matériel explosif, produits inflammables, sources de rayonnement électromagnétique ou thermique...) doivent être étudiés et pris en compte lors de l'installation des sites. |

**EF.MAT-INVENT**

| | |
|---|---|
| Description | Un inventaire global des biens et ressources (y compris les licences associées) permettant au moins d'identifier les éléments sensibles et vitaux, ainsi que leur localisation, doit être dressé et tenu à jour. |

**EF.MAT-MAINT**

| | |
|---|---|
| Description | Les installations, les matériels et les logiciels du système d'information ainsi que ceux qui assurent la protection du système d'information et la fourniture des services essentiels doivent être maintenus et testés régulièrement. |

**EF.MAT-PORTS**

| | |
|---|---|
| Description | L'accès aux ports de diagnostic doit être maîtrisé. |

**EF.ORG-ACCES-REVUE**

| | |
|---|---|
| Description | Un processus de revue des droits d'accès des utilisateurs doit être exécuté à des intervalles réguliers. |

**EF.ORG-ACCES-RH**

| | |
|---|---|
| Description | Des procédures doivent être formalisées et mises en oeuvre afin d'homogénéiser la gestion des ressources humaines et la base des habilitations et privilèges en tenant compte en fonction des besoins d'en connaître et d'en modifier. |

**EF.ORG-ACHATS**

| | |
|---|---|
| Description | L'achat, l'utilisation et la modification des matériels, supports et logiciels doivent être maîtrisés et contrôlés afin de les protéger contre la possibilité d'introduction de voies secrètes et de code de Troie.<br>Ils doivent systématiquement faire l'objet d'un contrat prenant en compte l'ergonomie et la maintenance. |

**EF.ORG-CHARGE**

| | |
|---|---|
| Description | Les personnels du cabinet d'études doivent systématiquement prendre en charge les matériels et logiciels qui lui sont confiés par le biais d'un formulaire signé. |

**EF.ORG-CONSIGN-IMPR**

| | |
|---|---|
| Description | Les consignes de sécurité en cas de sinistre doivent être imprimées sur un support qui attire l'œil |

**EF.ORG-CONSIGN-PUB**

| | |
|---|---|
| Description | Les consignes de sécurité en cas de sinistre doivent être affichées à hauteur d'homme dans des endroits dégagés en respectant les normes et standards en usage |

**EF.ORG-CONSIGN-PUB-SITE**

| | |
|---|---|
| Description | Les consignes de sécurité en cas de sinistre doivent être affichées en plusieurs endroits du site et notamment dans les endroits de passage et les endroits concernés par les consignes (ascenseur, installation susceptible de provoquer un dégât des eaux...) |

**EF.ORG-CONSIGN-REDAC**

| | |
|---|---|
| Description | Les consignes de sécurité en cas de sinistre doivent être rédigées de façon claire et lisible en respectant les normes et standards en usage |

**EF.ORG-CONTINUITE**

| | |
|---|---|
| Description | Le cabinet d'études doit formaliser un plan de continuité qui devra être régulièrement testé. |

**EF.ORG-CONTRATS**

| | |
|---|---|
| Description | Les contrats de services externalisés doivent définir les responsabilités des contractants et les recours possibles en cas de défaillances à cet accord. |

**EF.ORG-CONTROLE**

| | |
|---|---|
| Description | Le cabinet d'étude doit régulièrement effectuer un contrôle (recette, tests, contrôle hiérarchique, audit externe...) de la bonne application des règles de sécurité. |

**EF.ORG-CRISE**

| | |
|---|---|
| Description | Le cabinet d'études doit s'appuyer sur les moyens existants, sur la politique de sécurité et sur le plan de continuité pour détecter et gérer les crises. |

**EF.ORG-DATA-IDENT**

| | |
|---|---|
| Description | Les données devant faire l'objet d'un archivage doivent être identifiées dans des procédures d'archivage spécifiques. |

**EF.ORG-DATA-MODAL**

| | |
|---|---|
| Description | Les procédures d'archivage doivent indiquer les modalités d'archivage des données, les supports à utiliser, la fréquence des archivages ainsi que les procédures de gestion des supports d'archivage vierges et une fois les opérations d'archivage réalisées. |

**EF.ORG-DATA-RESP**

| | |
|---|---|
| Description | Les responsables de chaque opération d'archivage ainsi que leurs remplaçants doivent être clairement identifiés. |

**EF.ORG-DIMENS**

| | |
|---|---|
| Description | Les demandes en capacité doivent être surveillées et des prévisions sur les besoins de capacité futurs doivent être faites afin d'assurer la disponibilité d'une puissance de traitement et d'un stockage adéquats. |

**EF.ORG-IDENT**

| | |
|---|---|
| Description | Les personnels du cabinet d'études sont responsables de l'identification de la classification des documents qu'ils créent. |

**EF.ORG-INCENDIE-NORME**

| | |
|---|---|
| Description | L'organisation de lutte contre l'incendie doit être conforme aux normes et standards en vigueur |

**EF.ORG-INCIDENTS**

| | |
|---|---|
| Description | Une procédure de notification, de traitement et de suivi des incidents doit être mise en place. |

**EF.ORG-MENTION**

| | |
|---|---|
| Description | Tout document électronique ou papier doit comporter la mention visible de son niveau de confidentialité selon l'échelle de besoins définie pour le cabinet d'études. |

**EF.ORG-PC**

| | |
|---|---|
| Description | Le cabinet d'études doit formaliser la délivrance de certificat (et l'ensemble des exigences et procédures associée) sous la forme d'une politique de certification (PC).<br>Les services considérés sont le contrôle d'accès, la signature et le chiffrement. |

**EF.ORG-PSSI**

| | |
|---|---|
| Description | Le cabinet d'études doit formaliser une PSSI sur la base d'une analyse des risques SSI (utilisation des méthodes EBIOS et PSSI) et assurer une communication adaptée auprès de tous les acteurs internes et externes.<br>Cette PSSI doit être validée par le Directeur afin d'exprimer la volonté stratégique de sécuriser le système d'information. |

**EF.ORG-SAUV-LIC**

| | |
|---|---|
| Description | Les contrats de licence doivent être conservés à l'abris du feu et des autres sinistres susceptibles de les rendre inutilisables. |

**EF.ORG-UTIL-ENREG**

| | |
|---|---|
| Description | Il doit y avoir une procédure officielle d'enregistrement et de désenregistrement des utilisateurs pour l'octroi de l'accès à tous les systèmes et les services informatiques multi-utilisateurs. |

**EF.PER-CONFID**

| | |
|---|---|
| Description | Les employés doivent signer un accord de confidentialité comme faisant partie de leurs conditions initiales d'emploi. |

**EF.PER-DEPART**

| | |
|---|---|
| Description | |

| | |
|---|---|
| | préparé le plus tôt possible. |

**EF.PER-DOCS-ACCES**

| | |
|---|---|
| Description | Les manuels de maintenance, d'exploitation et d'utilisation des applications ainsi que les éventuelles documentations internes complémentaires sur le sujet doivent être accessibles aux acteurs concernés. |

**EF.PER-FORM-OUTILS**

| | |
|---|---|
| Description | Tous les employés de l'organisme et, le cas échéant, les utilisateurs extérieurs à l'organisme, doivent recevoir une formation appropriée sur l'utilisation des outils (notamment à la mise en production de nouveaux outils). |

**EF.PER-FORM-PSSI**

| | |
|---|---|
| Description | Tous les personnels du cabinet d'études doivent recevoir une formation appropriée et des mises à jour régulières sur la politique de sécurité et les procédures de l'organisme. |

**EF.PER-HABIL**

| | |
|---|---|
| Description | Les responsables de l'attribution des habilitations doivent être clairement identifiés en fonction des éléments sur lesquels portent les habilitations. |

**EF.PER-PRES**

| | |
|---|---|
| Description | Avant son départ, un titulaire partant doit former son successeur et le présenter à ses interlocuteurs habituels. |

**EF.PER-PROC-ACCES**

| | |
|---|---|
| Description | Les procédures de maintenance, d'exploitation et d'utilisations des applications doivent être accessibles aux acteurs concernés. |

**EF.PER-PROT**

| | |
|---|---|
| Description | En cas d'environnement général difficile, l'organisation doit mettre en place des mesures de protection du personnel (service de protection, hébergement proche du site...). |

**EF.PER-REMPL-FONC**

| | |
|---|---|
| Description | Les équipes doivent être dimensionnées pour pouvoir assurer leurs fonctions essentielles en cas d'indisponibilité d'une partie de leurs membres. |

**EF.PER-REMPL-FORM**

| | |
|---|---|
| Description | Les remplaçants identifiés pour prendre en charge des fonctions ponctuellement vacantes doivent être formés aux tâches associées à ces fonctions. |

**EF.PER-REMPL-INF**

| | |
|---|---|
| Description | Les remplaçants identifiés pour prendre en charge des fonctions ponctuellement vacantes doivent être informés des responsabilités associées à ces fonctions. |

**EF.PER-RESP-CONS**

| | |
|---|---|
| Description | Le responsable de la revue des consignes de sécurité de bon usage doit être clairement identifié |

**EF.PER-ROLES**

| | |
|---|---|
| Description | Les rôles et les responsabilités en matière de sécurité, tels qu'ils sont décrits dans la politique de sécurité de l'organisme doivent être documentés dans les définitions des postes dans la mesure du possible. |

**EF.PER-SENSIB**

| | |
|---|---|
| Description | L'ensemble des utilisateurs du système d'information doit être sensibilisé aux risques pesant sur le système d'information, aux problèmes de sécurité |

| | |
|---|---|
| | rôles et responsabilités. |
| **EF.PER-TRANSITION** | |
| Description | Une période de transition suffisamment longue doit être prévue pendant laquelle le titulaire partant et son successeur occupe les mêmes fonctions. |
| **EF.PHY-ACCUEIL** | |
| Description | Les personnes extérieures ne doivent pas pouvoir pénétrer sur le site ou en sortir sans passer par l'accueil. |
| **EF.PHY-ADAPT** | |
| Description | L'aménagement des locaux doit être le plus favorable possible au travail demandé (éclairage suffisant, température adaptée, isolation phonique, espace de rangement...). |
| **EF.PHY-DIMENS** | |
| Description | Les services essentiels et les secours doivent être dimensionnés de manière à offrir des services adaptés et de qualité y compris lors des éventuelles périodes de pointe. |

| EF.PHY-INCEND-DETEC | |
|---|---|
| Description | Les locaux doivent être équipés de dispositifs de détection et de lutte anti-incendie. |

| EF.PHY-INCEND-DETEC-ADAPT | |
|---|---|
| Description | Les dispositifs de détection et de lutte anti-incendie doivent être adaptés aux sites et zones d'implantation et dimensionné de façon adéquate. |

| EF.PHY-LOCALISATION | |
|---|---|
| Description | Le matériel informatique doit être situé et protégé de façon à réduire les risques présentés par les menaces et les dangers liés à l'environnement et les occasions d'accès non autorisés. |

| EF.PHY-NOM | |
|---|---|
| Description | Les normes d'installation de sites doivent définir une nomenclature de zonage physique permettant de réduire les impacts des sinistres (isolation de zone par porte coupe-feu par exemple). |

| EF.PHY-NORM | |
|---|---|
| Description | Les normes d'installation de sites doivent être basées sur les normes et les standards nationaux et/ou internationaux en vigueur pour la protection contre les sinistres (incendie, accident...). |

| EF.PHY-PREV | |
|---|---|
| Description | L'aménagement des locaux doit tenir compte des éléments qu'il est prévu d'y installer (contrôle de la température, surveillance de l'hygrométrie, filtrage de poussières ou autres éléments polluants...). |

| EF.PHY-PREV-VISIT | |
|---|---|
| Description | A partir de sa prise en charge, l'interlocuteur interne est responsable d'un visiteur jusqu'à son départ. Il doit notamment s'assurer que la visite se déroule en accord avec les principes de sécurité énoncés dans la politique de sécurité. |

| EF.PHY-RISQUES | |
|---|---|
| Description | Avant d'utiliser des services externes de gestion des infrastructures, les risques doivent être identifiés à l'avance et des mesures de maîtrise appropriées doivent être convenues avec le fournisseur et incluses dans le contrat. |

| EF.PHY.PER | |
|---|---|
| Description | Des dispositions spécifiques doivent être prises afin de réduire les perturbations sur le lieu de travail (pas de réunion dans des *open-space*, machine à café à l'écart des espaces de travail...). |

| EF.RES-ENTRE | |
|---|---|
| Description | Le matériel doit être entretenu conformément aux instructions du fabricant et/ou aux procédures documentées afin d'assurer sa disponibilité et son intégrité continues. |

### 7.1.2 Démonstration de la couverture

Les tableaux suivants présentent comment les exigences de sécurité fonctionnelles satisfont les 52 objectifs de sécurité.

La couleur orangée indique les éléments incomplètement couverts.

| O.LOG-AUTH | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-AUTH<br>EF.ORG-PC |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Les fonctions d'identification et d'authentification sont pleinement assurées et gérés par la mise en oeuvre d'une authentification forte et la formalisation d'une politique de certification. |

| O.LOG-CONF-SYS | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-CONTR |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Les contrôles de conformité périodiques permettent de garantir le respect des règles de la politique de sécurité. |

| O.LOG-HABIL | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-ACCES<br>EF.LOG-BESOINS<br>EF.LOG-PRIVIL<br>EF.LOG-SERVICES<br>EF.ORG-ACCES-REVUE<br>EF.ORG-ACCES-RH<br>EF.ORG-UTIL-ENREG<br>EF.PER-HABIL |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La mise en oeuvre des mécanismes de contrôle d'accès et une gestion cohérente avec la gestion des ressources humaines permet d'obtenir une gestion dynamique des habilitations. |

| O.LOG-LICEN | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.MAT-INVENT<br>EF.ORG-SAUV-LIC |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | L'inventaire des licences et leur conservation sûre permettent au cabinet d'études de respecter les lois en vigueur. |

| O.MAT-AMOR | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-CONFIG |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | L'interdiction matérielle et logicielle d'amorcer les postes à partir de périphériques amovibles satisfait l'objectif de sécurité. |

| O.MAT-AUTH-DOC | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-SIGNATURE<br>EF.ORG-PC |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La signature électronique et la formalisation d'une politique de sécurité permettent d'apporter le niveau de confiance nécessaire pour satisfaire l'objectif de sécurité. |

| O.MAT-DESCR | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.MAT-INVENT |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La description de tous les équipements informatiques et leur localisation à l'aide d'un inventaire permet de satisfaire l'objectif de sécurité au niveau requis. |

| O.MAT-DIV | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.PER-CONFID<br>EF.PER-SENSIB |
| Niveau de couverture | Couverture partielle |
| Justification de couverture par les exigences | La sensibilisation des personnels du cabinet d'études et leur engagement de responsabilité permettent d'éviter les divulgations involontaires d'informations sensibles.<br><br>Néanmoins, ce n'est suffisant pour traiter la divulgation volontaire (malveillante). |

| O.MAT-ERG | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-ACHATS |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La prise en compte contractuelle de l'ergonomie et de la maintenance dans l'achats des matériels, supports et logiciels permet de satisfaire l'objectif de sécurité au niveau requis. |

| O.MAT-PROT | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.MAT-ANTIVOL<br>EF.MAT-BUREAU<br>EF.MAT-INVENT<br>EF.ORG-CHARGE<br>EF.PER-SENSIB<br>EF.PHY-PREV-VISIT |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La protection des supports et matériels au sein du cabinet d'études est assurée par des mesures organisationnelles, techniques et de sensibilisation.<br>La responsabilisation et la sensibilisation des personnels permet de les protéger à l'extérieur de l'établissement. |

| O.MAT-REMP | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |

| | |
|---|---|
| Couverture | EF.ORG-ACHATS<br>EF.ORG-CONTINUITE |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | L'existence d'un plan de continuité et la prise en compte systématique de la maintenance dans les contrats d'achat de matériels permet de garantir leur disponibilité dans des délais conformes aux besoins de sécurité exprimés. |

**O.MAT-RESTAU**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-DOC<br>EF.LOG-SAUV<br>EF.ORG-CONTINUITE |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | L'existence d'un plan de continuité prenant en compte la sauvegarde des informations métier et système, ainsi que des applications, permet d'assurer la remise en service logique du système d'information dans les délais conformes aux besoins de sécurité exprimés. |

**O.ORG-ARCHIV**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-ARCHIV-CONTR<br>EF.ORG-DATA-IDENT<br>EF.ORG-DATA-MODAL<br>EF.ORG-DATA-RESP<br>EF.ORG-PC |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La formalisation de procédures d'archivage et le recours à la signature électronique sur la base d'une politique de certification garantissent une gestion intègre de l'archivage. |

**O.ORG-CONF**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-CONTROLE<br>EF.ORG-IDENT<br>EF.ORG-MENTION |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les | L'identification de la classification des documents par les personnels du cabinet d'études et un contrôle régulier permettent de satisfaire l'objectif de sécurité au |

| | |
|---|---|
| exigences | niveau requis. |
| **O.ORG-CONSIGN** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-CONSIGN-IMPR<br>EF.ORG-CONSIGN-PUB<br>EF.ORG-CONSIGN-PUB-SITE<br>EF.ORG-CONSIGN-REDAC<br>EF.ORG-CONTROLE<br>EF.ORG-INCENDIE-NORME<br>EF.ORG-INCIDENTS<br>EF.PER-RESP-CONS |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La formalisation de procédures en cas d'incendie ou incident, leur communication auprès des personnels du cabinet d'études et leur contrôle régulier permettent de s'assurer que les consignes de sécurité seront respectées en cas d'incident ou de malveillance. |
| **O.ORG-CONT-OBJ** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-TRACES-DETEC<br>EF.LOG-TRACES-GEN<br>EF.ORG-CONTROLE |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La méthodologie employée pour déterminer les exigences de sécurité garantit leur adéquation aux objectifs de sécurité identifiés. Cette démarche, complétée par des mesures de contrôle, permet de satisfaire l'objectif de sécurité au niveau requis. |
| **O.ORG-CRISE** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-CRISE |
| Niveau de couverture | Couverture partielle |
| Justification de couverture par les exigences | L'organisation garantit une réaction rapide et efficace en cas de crise assurant une réduction des impacts potentiels et la continuité des activités essentielles : panne, sinistre, intrusion majeure, autre malveillance.<br><br>Il n'existera cependant pas de plan formalisant l'organisation et la communication relative à la crise, ce qui peut conduire à une mauvaise gestion de cette crise (communication inadaptée, impact aggravé...). |

| O.ORG-EQMT | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-FILTRE<br>EF.MAT-MAINT<br>EF.ORG-ACHATS<br>EF.ORG-DIMENS<br>EF.PER-DOCS-ACCES<br>EF.PER-PROC-ACCES<br>EF.PHY-DIMENS |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Les analyses de dimensionnement, le filtrage des flux et la contractualisation de la maintenance permettent de prévenir la saturation et les pannes des équipements (informatiques, climatisation, énergie, communication). |

| O.ORG-EXIG | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-CONTROLE<br>EF.PER-ROLES |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La définition des rôles et responsabilités, ainsi que des contrôles réguliers de l'application des règles de sécurité permettent de garantir que les exigences minimales de sécurité des systèmes d'information sont respectées de tous. |

| O.ORG-MAINTIEN | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.MAT-INVENT<br>EF.MAT-MAINT<br>EF.ORG-ACHATS<br>EF.ORG-INCIDENTS<br>EF.RES-ENTRE |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La contractualisation de la maintenance, l'entretien des ressources, l'inventaire des ressources et la remontée d'incidents permettent de s'assurer que tout matériel ou logiciel est maintenu. |

| O.ORG-MOY | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.MAT-DIM<br>EF.MAT-MAINT<br>EF.ORG-ACHATS<br>EF.ORG-CONTINUITE |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Le dimensionnement, la maintenance des ressources et les procédures relatives à la continuité des activités permettent de garantir que les moyens de secours sont opérationnels et assurent si cela est possible la continuité de service des activités sensibles de l'organisme en cas de panne, de sinistre ou de malveillance majeure. |

| O.ORG-POL-SYS | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-USAGE<br>EF.ORG-CONTROLE |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La mise en place d'une procédure de recette permet de garantir le respect de la politique de sécurité lors de la mise en place de tout système sensible (matériel ou logiciel). |

| O.ORG-POL-SYS-SENS | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-CONTROLE<br>EF.PER-FORM-PSSI<br>EF.PER-RESP-CONS<br>EF.PER-ROLES<br>EF.PER-SENSIB |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La définition des rôles et responsabilités, la sensibilisation et la formation, ainsi que le contrôle de la mise en oeuvre des règles de sécurité permettent de faire respecter les exigences de la politique de sécurité dans le développement, l'usage et l'exploitation des systèmes (matériels et logiciels). |

| O.ORG-PREUV | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-TRACES-DETEC<br>EF.LOG-TRACES-EXPL<br>EF.LOG-TRACES-GEN<br>EF.LOG-TRACES-STOCK<br>EF.ORG-CONTROLE |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La gestion sécurisée des traces et son contrôle permettent de s'assurer que les traces et les éléments de preuves sont exploités et protégés en accord avec la politique de sécurité. |

| O.ORG-PSSI | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-PSSI |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | L'utilisation d'une méthode de gestion des risques SSI (EBIOS) et d'une méthode d'élaboration de PSSI permet au cabinet d'études de disposer d'une PSSI en adéquation avec ses besoins. |

| O.ORG-REGLEMENT | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-PSSI |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | L'utilisation d'une méthode de gestion des risques SSI (EBIOS) et d'une méthode d'élaboration de PSSI permet au cabinet d'études de disposer d'une PSSI en adéquation avec ses besoins, notamment de prendre en compte la réglementation applicable. |

| O.ORG-ROLES | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-PSSI<br>EF.PER-DOCS-ACCES |

| | |
|---|---|
| | EF.PER-PROC-ACCES<br>EF.PER-ROLES |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La PSSI constitue la référence en matière de SSI pour l'ensemble des personnels du cabinet d'études. Elle permet de garantir que chaque rôle lié à la sécurité du système d'information doit toujours (même en cas d'absence du titulaire) être placé sous la responsabilité d'au moins une personne ayant les compétences requises ou la possibilité de se référer à une documentation adéquate. La définition des rôles et responsabilités complète la satisfaction de l'objectif de sécurité. |
| **O.ORG-SAUV** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-DOC<br>EF.LOG-SAUV<br>EF.ORG-CONTINUITE<br>EF.ORG-SAUV-LIC |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La mise en place d'un plan de continuité et des moyens de sauvegarde en cohérence permet de s'assurer que toutes les données sont sauvegardées selon une fréquence adéquate (y compris des données non centralisées). |
| **O.ORG-SSTRAIT** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-USAGE<br>EF.ORG-CONTRATS<br>EF.ORG-PSSI<br>EF.PHY-PREV-VISIT<br>EF.PHY-RISQUES |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La définition de clauses contractuelles, de procédures organisationnelles et techniques propres à l'intervention de tiers, ainsi qu'une communication appropriée au sujet de la PSSI permettent de s'assurer que ses sous-traitants/prestataires/fournisseurs/industriels/organisations filles/sites respectent la politique de sécurité lors de leurs interventions (travaux, développement, maintenance...). |
| **O.ORG-SUIV-INCID** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-INCIDENTS |

| | |
|---|---|
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Une procédure de notification, de traitement et de suivi des incidents permet de satisfaire l'objectif de sécurité au niveau requis. |

**O.ORG-TRANS**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-CHIFFREMENT<br>EF.LOG-SIGNATURE<br>EF.ORG-PC<br>EF.ORG-PSSI<br>EF.PER-SENSIB |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Le chiffrement et la signature électronique sur la base de certificats et reposant sur une politique de certification, ainsi que la sensibilisation des personnels et l'élaboration d'une PSSI permettent de garantir la protection du contenu des moyens de transmission (selon leur nature) et de leur exploitation contre les risques de divulgation, de vol, d'altération, de répudiation et de perte. |

**O.ORG-TRAV**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.PER-PROT<br>EF.PHY-ADAPT<br>EF.PHY.PER |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Les mesures organisationnelles en cohérence avec le contexte et le personnel du cabinet d'études permettent de s'assurer que les conditions de travail sont satisfaisantes. |

**O.ORG-VIRUS**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-DOC<br>EF.LOG-MESSAGERIE<br>EF.LOG-ORIGINE<br>EF.LOG-POSTES<br>EF.LOG-SAUV<br>EF.LOG-USAGE<br>EF.LOG-VIRUS-DETEC<br>EF.ORG-ACHATS<br>EF.ORG-CONTINUITE<br>EF.ORG-PSSI |

| | |
|---|---|
| | EF.PER-SENSIB |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Un ensemble de mesures organisationnelles et techniques relatives à la prévention et à la détection des virus permet d'empêcher l'introduction et la diffusion dans les systèmes de code malveillant. |
| **O.ORG-VOL** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.PHY-ACCUEIL<br>EF.PHY-LOCALISATION<br>EF.PHY-PREV-VISIT |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | L'obligation du passage par l'accueil et l'accompagnement des tiers dans les locaux constituent des procédures d'entrées-sorties satisfaisantes pour lutter contre le vol de matériel au niveau de sécurité requis. |
| **O.PER-ADHES** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.PER-CONFID<br>EF.PER-FORM-PSSI<br>EF.PER-REMPL-FORM<br>EF.PER-REMPL-INF<br>EF.PER-ROLES<br>EF.PER-SENSIB |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La définition claire des rôles et responsabilités, ainsi que l'information, la sensibilisation et la formation des personnels et des éventuels personnels de remplacement permettent de faire en sorte que le personnel adhère à la démarche sécurité et connaisse les rôles et responsabilités. |
| **O.PER-IMP** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-PSSI |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La validation de la PSSI par le Directeur démontre son implication dans la démarche sécurité. |

| O.PER-INCID | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-CONTROLE<br>EF.ORG-INCIDENTS<br>EF.PER-FORM-PSSI |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | L'existence d'une procédure de remontée d'incident, la formation des personnels et les contrôles réguliers leur permettent de montrer des réactions réflexes en cas d'incident (devoir d'information, moyens de remontée de l'information...). |

| O.PER-NORME | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.PER-FORM-PSSI<br>EF.PER-SENSIB |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La sensibilisation et la formation des personnels du cabinet d'études permettent de satisfaire l'objectif de sécurité au niveau requis. |

| O.PER-POL | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.PER-DEPART<br>EF.PER-DOCS-ACCES<br>EF.PER-FORM-OUTILS<br>EF.PER-FORM-PSSI<br>EF.PER-PRES<br>EF.PER-PROC-ACCES<br>EF.PER-TRANSITION |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La préparation des départs et arrivées de personnels, notamment par la sensibilisation, permet aux nouveaux personnels ou remplaçants d'assurer leurs tâches en respect de la politique de sécurité. |

| O.PER-RESP | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence |

| | |
|---|---|
| résistance | relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-PSSI<br>EF.PER-CONFID<br>EF.PER-FORM-PSSI<br>EF.PER-ROLES<br>EF.PER-SENSIB |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La définition claire des rôles et responsabilités, des règles de sécurité, la formation des personnels et l'engagement de responsabilité permettent de les responsabiliser et de les informer des sanctions encourues. |

**O.PER-SEC**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-PSSI<br>EF.PER-CONFID<br>EF.PER-FORM-PSSI<br>EF.PER-ROLES<br>EF.PER-SENSIB |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | La définition claire des rôles et responsabilités, des règles de sécurité, la formation des personnels et l'engagement de responsabilité permettent de les sensibiliser au respect du secret professionnel et de la discrétion. |

**O.PER-SENSIB**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.PER-CONFID<br>EF.PER-FORM-PSSI<br>EF.PER-ROLES<br>EF.PER-SENSIB |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Les personnels ayant accès à des informations sensibles sont sensibilisés et identifiés par un ensemble de mesures de sensibilisation, formation et définition des rôles. |

**O.PER-USAGE**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-CONTROLE<br>EF.PER-FORM-OUTILS<br>EF.PER-FORM-PSSI<br>EF.PER-ROLES |

| | |
|---|---|
| | EF.PER-SENSIB |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Les rôles et responsabilités étant identifiés, les personnels sensibilisés et formés, et l'application de la politique de sécurité étant contrôlée, cela permet aux personnels de respecter les bons usages de l'outil informatique, des moyens de communication et de la manipulation des supports ainsi que les dispositions de sécurité associées à la classification des informations. |

**O.PER-VOL**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-AUTH<br>EF.LOG-CHIFFREMENT<br>EF.LOG-CONTR<br>EF.MAT-EXT<br>EF.ORG-CHARGE<br>EF.PER-FORM-PSSI<br>EF.PER-SENSIB |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Un ensemble de mesures techniques (authentification, chiffrement, contrôles périodiques...) et organisationnelles (sensibilisation, prise en charge...) permet d'assurer la protection contre le vol ou l'intrusion des équipements et supports à l'extérieur des locaux la protection. |

**O.PER-VOLANT**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.PER-REMPL-FONC<br>EF.PER-REMPL-FORM<br>EF.PER-REMPL-INF |
| Niveau de couverture | Couverture partielle |
| Justification de couverture par les exigences | La gestion du remplacement de personnels est envisageable dans la limite des moyens du cabinet d'études.<br><br>Un trop grand nombre de remplacements n'est pas envisageable. |

**O.PHY-ACCES**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.MAT-ANTIVOL<br>EF.MAT-BUREAU<br>EF.PHY-ACCUEIL |

| | |
|---|---|
| | EF.PHY-PREV-VISIT |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Le passage obligatoire des visiteurs par l'accueil permet de contrôler l'accès au cabinet d'études. L'accompagnement systématique des visiteurs et des mesures de protection des matériels et supports permettent de compléter cette exigence. |
| **O.PHY-INCEND** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.PHY-INCEND-DETEC<br>EF.PHY-INCEND-DETEC-ADAPT<br>EF.PHY-NOM<br>EF.PHY-NORM |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Des mesures adaptées de détection et de lutte contre l'incendie, ainsi que le respect des normes en vigueur permettent de satisfaire l'objectif de sécurité au niveau requis. |
| **O.PHY-MAT-DANG** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.MAT-INSTALL<br>EF.PHY-NOM |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | L'étude des risques spécifiques et des mesures de protection physiques permettent de satisfaire l'objectif de sécurité au niveau requis. |
| **O.PHY-NORME** | |
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.ORG-PSSI<br>EF.PHY-NORM |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Le respect des normes en vigueur et de la PSSI permet de satisfaire l'objectif de sécurité au niveau requis. |
| **O.RES-INT** | |
| Niveau de résistance | 2 |

| | |
|---|---|
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-FILTRE<br>EF.LOG-PRIVIL<br>EF.LOG-SERVICES<br>EF.MAT-PORTS<br>EF.PHY-ACCUEIL<br>EF.PHY-LOCALISATION<br>EF.PHY-PREV-VISIT |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Les exigences de sécurité physique et de sécurité logique déterminées permettent de satisfaire l'objectif de sécurité au niveau requis. |

**O.PHY-SERVICES**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.MAT-MAINT<br>EF.PER-FORM-OUTILS<br>EF.PHY-DIMENS<br>EF.PHY-PREV<br>EF.PHY-RISQUES<br>EF.RES-ENTRE |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Les mesures de prévention prévues permettent de satisfaire l'objectif de sécurité au niveau requis. |

**O.RES-TRANS**

| | |
|---|---|
| Niveau de résistance | 2 |
| Justification du niveau de résistance | Décision du comité de pilotage sur la base des risques concernés (notamment du potentiel d'attaque des éléments menaçants) et d'une mise en cohérence relative avec les autres objectifs de sécurité. |
| Couverture | EF.LOG-AUTH<br>EF.LOG-CHIFFREMENT<br>EF.LOG-CONTR<br>EF.LOG-FILTRE<br>EF.LOG-PRIVIL<br>EF.LOG-SERVICES<br>EF.MAT-PORTS<br>EF.ORG-DIMENS<br>EF.ORG-PC |
| Niveau de couverture | Couverture complète |
| Justification de couverture par les exigences | Les exigences techniques et non techniques prévues permettent de protéger les transmissions en confidentialité, intégrité et disponibilité. |

### 7.1.3 Justification des exigences de sécurité fonctionnelles

Les tableaux-croisés ci-dessous démontrent que chaque exigence de sécurité fonctionnelle répond au moins à un objectif de sécurité.
La couleur orangée indique les éléments incomplètement couverts.

1ère partie des exigences de sécurité fonctionnelles :

| | EF.LOG-ACCES | EF.LOG-ARCHIV-CONTR | EF.LOG-AUTH | EF.LOG-BESOINS | EF.LOG-CHIFFREMENT | EF.LOG-CONFIG | EF.LOG-CONTR | EF.LOG-DOC | EF.LOG-FILTRE | EF.LOG-MESSAGERIE | EF.LOG-ORIGINE | EF.LOG-POSTES | EF.LOG-PRIVIL | EF.LOG-SAUV | EF.LOG-SERVICES | EF.LOG-SIGNATURE | EF.LOG-TRACES-DETEC | EF.LOG-TRACES-EXPL | EF.LOG-TRACES-GEN | EF.LOG-TRACES-STOCK | EF.LOG-USAGE | EF.LOG-VIRUS-DETEC | EF.MAT-ANTIVOL | EF.MAT-BUREAU | EF.MAT-DIM | EF.MAT-EXT | EF.ORG-PC | EF.ORG-PSSI |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.LOG-AUTH | | | X | | | | | | | | | | | | | | | | | | | | | | | | X | |
| O.LOG-CONF-SYS | | | | | | | X | | | | | | | | | | | | | | | | | | | | | |
| O.LOG-HABIL | X | | | X | | | | | | | | | X | | X | | | | | | | | | | | | | |
| O.LOG-LICEN | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.MAT-AMOR | | | | | | X | | | | | | | | | | | | | | | | | | | | | | |
| O.MAT-AUTH-DOC | | | | | | | | | | | | | | | | X | | | | | | | | | | | X | |
| O.MAT-DESCR | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.MAT-DIV | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.MAT-ERG | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.MAT-PROT | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | |
| O.MAT-REMP | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.MAT-RESTAU | | | | | | | | X | | | | | | X | | | | | | | | | | | | | | |
| O.ORG-ARCHIV | | X | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| O.ORG-CONF | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-CONSIGN | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-CONT-OBJ | | | | | | | | | | | | | | | | | X | | X | | | | | | | | | |
| O.ORG-CRISE | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-EQMT | | | | | | | | | X | | | | | | | | | | | | | | | | | | | |
| O.ORG-EXIG | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-MAINTIEN | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-MOY | | | | | | | | | | | | | | | | | | | | | | | | | X | | | |
| O.ORG-POL-SYS | | | | | | | | | | | | | | | | | | | | | X | | | | | | | |
| O.ORG-POL-SYS-SENS | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-PREUV | | | | | | | | | | | | | | | | | X | X | X | X | | | | | | | | |
| O.ORG-PSSI | | | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| O.ORG-REGLEMENT | | | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| O.ORG-ROLES | | | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| O.ORG-SAUV | | | | | | | | X | | | | | | X | | | | | | | | | | | | | | |
| O.ORG-SSTRAIT | | | | | | | | | | | | | | | | | | | | | X | | | | | | | X |
| O.ORG-SUIV-INCID | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-TRANS | | | | | X | | | | | | | | | | | X | | | | | | | | | | | X | X |
| O.ORG-TRAV | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-VIRUS | | | | | | | | X | | X | X | X | | X | | | | | | | X | X | | | | | | X |
| O.ORG-VOL | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

| | EF.LOG-ACCES | EF.LOG-ARCHIV-CONTR | EF.LOG-AUTH | EF.LOG-BESOINS | EF.LOG-CHIFFREMENT | EF.LOG-CONFIG | EF.LOG-CONTR | EF.LOG-DOC | EF.LOG-FILTRE | EF.LOG-MESSAGERIE | EF.LOG-ORIGINE | EF.LOG-POSTES | EF.LOG-PRIVIL | EF.LOG-SAUV | EF.LOG-SERVICES | EF.LOG-SIGNATURE | EF.LOG-TRACES-DETEC | EF.LOG-TRACES-EXPL | EF.LOG-TRACES-GEN | EF.LOG-TRACES-STOCK | EF.LOG-USAGE | EF.LOG-VIRUS-DETEC | EF.MAT-ANTIVOL | EF.MAT-BUREAU | EF.MAT-DIM | EF.MAT-EXT | EF.ORG-PC | EF.ORG-PSSI |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.PER-ADHES | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PER-IMP | | | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| O.PER-INCID | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PER-NORME | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PER-POL | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PER-RESP | | | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| O.PER-SEC | | | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| O.PER-SENSIB | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PER-USAGE | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PER-VOL | | | X | | X | | X | | | | | | | | | | | | | | | | | | | X | | |
| O.PER-VOLANT | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PHY-ACCES | | | | | | | | | | | | | | | | | | | | | | | X | X | | | | |
| O.PHY-INCEND | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PHY-MAT-DANG | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PHY-NORME | | | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| O.RES-INT | | | | | | | | | X | | | | X | | X | | | | | | | | | | | | | |
| O.PHY-SERVICES | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.RES-TRANS | | | X | | X | | X | | X | | | | X | | X | | | | | | | | | | | | X | |

2nde partie des exigences de sécurité fonctionnelles :

| | EF.MAT-INSTALL | EF.MAT-INVENT | EF.MAT-MAINT | EF.MAT-PORTS | EF.ORG-ACCES-REVUE | EF.ORG-ACCES-RH | EF.ORG-ACHATS | EF.ORG-CHARGE | EF.ORG-CONSIGN-IMPR | EF.ORG-CONSIGN-PUB | EF.ORG-CONSIGN-PUB-SITE | EF.ORG-CONSIGN-REDAC | EF.ORG-CONTINUITE | EF.ORG-CONTRATS | EF.ORG-CONTROLE | EF.ORG-CRISE | EF.ORG-DATA-IDENT | EF.ORG-DATA-MODAL | EF.ORG-DATA-RESP | EF.ORG-DIMENS | EF.ORG-IDENT | EF.ORG-INCENDIE-NORME | EF.ORG-INCIDENTS | EF.ORG-MENTION | EF.ORG-SAUV-LIC | EF.ORG-UTIL-ENREG | EF.PER-CONFID | EF.PER-DEPART |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.LOG-AUTH | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.LOG-CONF-SYS | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.LOG-HABIL | | | | | X | X | | | | | | | | | | | | | | | | | | | | X | | |
| O.LOG-LICEN | | X | | | | | | | | | | | | | | | | | | | | | | | X | | | |
| O.MAT-AMOR | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.MAT-AUTH-DOC | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.MAT-DESCR | | X | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.MAT-DIV | | | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| O.MAT-ERG | | | | | | | X | | | | | | | | | | | | | | | | | | | | | |
| O.MAT-PROT | | X | | | | | | X | | | | | | | | | | | | | | | | | | | | |
| O.MAT-REMP | | | | | | | X | | | | | | X | | | | | | | | | | | | | | | |

| | EF.MAT-INSTALL | EF.MAT-INVENT | EF.MAT-MAINT | EF.MAT-PORTS | EF.ORG-ACCES-REVUE | EF.ORG-ACCES-RH | EF.ORG-ACHATS | EF.ORG-CHARGE | EF.ORG-CONSIGN-IMPR | EF.ORG-CONSIGN-PUB | EF.ORG-CONSIGN-PUB-SITE | EF.ORG-CONSIGN-REDAC | EF.ORG-CONTINUITE | EF.ORG-CONTRATS | EF.ORG-CONTROLE | EF.ORG-CRISE | EF.ORG-DATA-IDENT | EF.ORG-DATA-MODAL | EF.ORG-DATA-RESP | EF.ORG-DIMENS | EF.ORG-IDENT | EF.ORG-INCENDIE-NORME | EF.ORG-INCIDENTS | EF.ORG-MENTION | EF.ORG-SAUV-LIC | EF.ORG-UTIL-ENREG | EF.PER-CONFID | EF.PER-DEPART |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.MAT-RESTAU | | | | | | | | | | | | | X | | | | | | | | | | | | | | | |
| O.ORG-ARCHIV | | | | | | | | | | | | | | | | | X | X | X | | | | | | | | | |
| O.ORG-CONF | | | | | | | | | | | | | | | X | | | | | | X | | | X | | | | |
| O.ORG-CONSIGN | | | | | | | | | X | X | X | X | | | X | | | | | | | X | X | | | | | |
| O.ORG-CONT-OBJ | | | | | | | | | | | | | | | X | | | | | | | | | | | | | |
| O.ORG-CRISE | | | | | | | | | | | | | | | | X | | | | | | | | | | | | |
| O.ORG-EQMT | | | X | | | | X | | | | | | | | | | | | | X | | | | | | | | |
| O.ORG-EXIG | | | | | | | | | | | | | | | X | | | | | | | | | | | | | |
| O.ORG-MAINTIEN | | X | X | | | | X | | | | | | | | | | | | | | | | X | | | | | |
| O.ORG-MOY | | | X | | | | X | | | | | | X | | | | | | | | | | | | | | | |
| O.ORG-POL-SYS | | | | | | | | | | | | | | | X | | | | | | | | | | | | | |
| O.ORG-POL-SYS-SENS | | | | | | | | | | | | | | | X | | | | | | | | | | | | | |
| O.ORG-PREUV | | | | | | | | | | | | | | | X | | | | | | | | | | | | | |
| O.ORG-PSSI | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-REGLEMENT | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-ROLES | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-SAUV | | | | | | | | | | | | | X | | | | | | | | | | | | X | | | |
| O.ORG-SSTRAIT | | | | | | | | | | | | | | X | | | | | | | | | | | | | | |
| O.ORG-SUIV-INCID | | | | | | | | | | | | | | | | | | | | | | | X | | | | | |
| O.ORG-TRANS | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-TRAV | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.ORG-VIRUS | | | | | | | X | | | | | | X | | | | | | | | | | | | | | | |
| O.ORG-VOL | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PER-ADHES | | | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| O.PER-IMP | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PER-INCID | | | | | | | | | | | | | | | X | | | | | | | | X | | | | | |
| O.PER-NORME | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PER-POL | | | | | | | | | | | | | | | | | | | | | | | | | | | | X |
| O.PER-RESP | | | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| O.PER-SEC | | | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| O.PER-SENSIB | | | | | | | | | | | | | | | | | | | | | | | | | | | X | |
| O.PER-USAGE | | | | | | | | | | | | | | | X | | | | | | | | | | | | | |
| O.PER-VOL | | | | | | | | X | | | | | | | | | | | | | | | | | | | | |
| O.PER-VOLANT | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PHY-ACCES | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PHY-INCEND | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PHY-MAT-DANG | X | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PHY-NORME | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.RES-INT | | | | X | | | | | | | | | | | | | | | | | | | | | | | | |
| O.PHY-SERVICES | | | X | | | | | | | | | | | | | | | | | | | | | | | | | |
| O.RES-TRANS | | | | X | | | | | | | | | | | | | | | | X | | | | | | | | |

3ème partie des exigences de sécurité fonctionnelles :

| | EF.PER-DOCS-ACCES | EF.PER-FORM-OUTILS | EF.PER-FORM-PSSI | EF.PER-HABIL | EF.PER-PRES | EF.PER-PROC-ACCES | EF.PER-PROT | EF.PER-REMPL-FONC | EF.PER-REMPL-FORM | EF.PER-REMPL-INF | EF.PER-RESP-CONS | EF.PER-ROLES | EF.PER-SENSIB | EF.PER-TRANSITION | EF.PHY-ACCUEIL | EF.PHY-ADAPT | EF.PHY-DIMENS | EF.PHY-INCEND-DETEC | EF.PHY-INCEND-DETEC-ADAPT | EF.PHY-LOCALISATION | EF.PHY-NOM | EF.PHY-NORM | EF.PHY-PREV | EF.PHY-PREV-VISIT | EF.PHY-RISQUES | EF.PHY.PER | EF.RES-ENTRE | Couverture |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.LOG-AUTH | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.LOG-CONF-SYS | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.LOG-HABIL | | | | X | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.LOG-LICEN | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.MAT-AMOR | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.MAT-AUTH-DOC | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.MAT-DESCR | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.MAT-DIV | | | | | | | | | | | | | X | | | | | | | | | | | | | | | 1 |
| O.MAT-ERG | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.MAT-PROT | | | | | | | | | | | | | X | | | | | | | | | | | X | | | | 2 |
| O.MAT-REMP | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.MAT-RESTAU | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-ARCHIV | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-CONF | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-CONSIGN | | | | | | | | | | | X | | | | | | | | | | | | | | | | | 2 |
| O.ORG-CONT-OBJ | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-CRISE | | | | | | | | | | | | | | | | | | | | | | | | | | | | 1 |
| O.ORG-EQMT | X | | | | | X | | | | | | | | | | | X | | | | | | | | | | | 2 |
| O.ORG-EXIG | | | | | | | | | | | | X | | | | | | | | | | | | | | | | 2 |
| O.ORG-MAINTIEN | | | | | | | | | | | | | | | | | | | | | | | | | | | X | 2 |
| O.ORG-MOY | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-POL-SYS | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-POL-SYS-SENS | | | X | | | | | | | | X | X | X | | | | | | | | | | | | | | | 2 |
| O.ORG-PREUV | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-PSSI | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-REGLEMENT | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-ROLES | X | | | X | | X | | | | | | X | | | | | | | | | | | | | | | | 2 |
| O.ORG-SAUV | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-SSTRAIT | | | | | | | | | | | | | | | | | | | | | | | | X | X | | | 2 |
| O.ORG-SUIV-INCID | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.ORG-TRANS | | | | | | | | | | | | | X | | | | | | | | | | | | | | | 2 |
| O.ORG-TRAV | | | | | | | X | | | | | | | | | X | | | | | | | | | | X | | 2 |
| O.ORG-VIRUS | | | | | | | | | | | | | X | | | | | | | | | | | | | | | 2 |
| O.ORG-VOL | | | | | | | | | | | | | | | X | | | | | X | | | | X | | | | 2 |
| O.PER-ADHES | | | X | | | | | | X | X | | X | X | | | | | | | | | | | | | | | 2 |
| O.PER-IMP | | | | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.PER-INCID | | | X | | | | | | | | | | | | | | | | | | | | | | | | | 2 |
| O.PER-NORME | | | X | | | | | | | | | | X | | | | | | | | | | | | | | | 2 |
| O.PER-POL | X | X | X | | X | X | | | | | | | | X | | | | | | | | | | | | | | 2 |
| O.PER-RESP | | | X | | | | | | | | | X | X | | | | | | | | | | | | | | | 2 |
| O.PER-SEC | | | X | | | | | | | | | X | X | | | | | | | | | | | | | | | 2 |
| O.PER-SENSIB | | | X | | | | | | | | | X | X | | | | | | | | | | | | | | | 2 |

| | EF.PER-DOCS-ACCES | EF.PER-FORM-OUTILS | EF.PER-FORM-PSSI | EF.PER-HABIL | EF.PER-PRES | EF.PER-PROC-ACCES | EF.PER-PROT | EF.PER-REMPL-FONC | EF.PER-REMPL-FORM | EF.PER-REMPL-INF | EF.PER-RESP-CONS | EF.PER-ROLES | EF.PER-SENSIB | EF.PER-TRANSITION | EF.PHY-ACCUEIL | EF.PHY-ADAPT | EF.PHY-DIMENS | EF.PHY-INCEND-DETEC | EF.PHY-INCEND-DETEC-ADAPT | EF.PHY-LOCALISATION | EF.PHY-NOM | EF.PHY-NORM | EF.PHY-PREV | EF.PHY-PREV-VISIT | EF.PHY-RISQUES | EF.PHY.PER | EF.RES-ENTRE | **Couverture** |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| O.PER-USAGE | | X | X | | | | | | | | | X | X | | | | | | | | | | | | | | | **2** |
| O.PER-VOL | | | X | | | | | | | | | | X | | | | | | | | | | | | | | | **2** |
| O.PER-VOLANT | | | | | | | | X | X | X | | | | | | | | | | | | | | | | | | **1** |
| O.PHY-ACCES | | | | | | | | | | | | | | | X | | | | | X | | | | X | | | | **2** |
| O.PHY-INCEND | | | | | | | | | | | | | | | | | | X | X | | X | X | | | | | | **2** |
| O.PHY-MAT-DANG | | | | | | | | | | | | | | | | | | | | | X | | | | | | | **2** |
| O.PHY-NORME | | | | | | | | | | | | | | | | | | | | | | X | | | | | | **2** |
| O.RES-INT | | | | | | | | | | | | | | | X | | | | | X | | | | X | | | | **2** |
| O.PHY-SERVICES | | X | | | | | | | | | | | | | | | X | | | | | | X | | X | | X | **2** |
| O.RES-TRANS | | | | | | | | | | | | | | | | | | | | | | | | | | | | **2** |

## 7.2 Activité 2 : Détermination des exigences de sécurité d'assurance

*La dernière activité de la démarche consiste à déterminer les exigences de sécurité d'assurance.*

*Ces exigences permettent d'améliorer la confiance envers la conception et la mise en œuvre de la sécurité du système.*

*L'ISO/IEC 15408 définit 7 niveaux d'assurance correspondant à des paquets d'exigences de sécurité d'assurance. Plus le niveau augmente, plus la confiance envers la conception et la mise en œuvre de la sécurité est garantie car le niveau des exigences augmente.*

*Si l'un de ces niveaux a été choisi, cette activité ne consiste qu'à extraire et éventuellement reformuler les exigences de sécurité d'assurance correspondant à ce niveau dans l'étude. Leur "consistance" (cohérence et dépendances) est démontrée dans l'ISO/IEC 15408.*

*Si ce n'est pas le cas, il est possible de rédiger de toute pièce ou d'extraire de l'ISO/IEC 15408 des exigences de sécurité d'assurance, dans la mesure où la "consistance" de l'ensemble des exigences est démontrée*

*Il est toujours possible d'en ajouter de nouvelles dans la mesure où la "consistance" de l'ensemble des exigences est démontrée.*

### 7.2.1 Formalisation des exigences de sécurité d'assurance

| EA.DEMONSTRATION | |
|---|---|
| Description | Une démonstration de correspondance informelle doit être effectuée entre les différents niveaux de représentation des fonctions de sécurité du système-cible. |

| EA.GUIDE-ADMIN | |
|---|---|
| Description | Le cabinet d'études doit disposer d'un guide de l'administrateur à l'attention du personnel chargé de l'administration du système.<br>Ce guide doit :<br><br>- Décrire les fonctions et les interfaces d'administration à la disposition de l'administrateur du système-cible ;<br>- Décrire comment administrer le système-cible d'une façon sûre ;<br>- Contenir des avertissements concernant les fonctions et les privilèges qui devraient être contrôlés dans un environnement d'exploitation sûr ;<br>- Décrire toutes les hypothèses relatives au comportement de l'utilisateur, qui ont un rapport avec l'exploitation sûre du système-cible ;<br>- Décrire tous les paramètres de sécurité qui sont sous le contrôle de l'administrateur, en indiquant les valeurs sûres quand cela est approprié ;<br>- Chaque type d'événement touchant à la sécurité, relatif aux fonctions d'administration qui doivent être réalisées, y compris le changement des caractéristiques de sécurité d'entités qui sont sous le contrôle des fonctions de sécurité ;<br>- Etre cohérent avec tous les autres documents fournis ;<br>- Décrire toutes les exigences de sécurité pour l'environnement TI, qui concernent l'administrateur. |

| EA.GUIDE-UTIL | |
|---|---|
| Description | Le cabinet d'études doit disposer d'un guide de l'utilisateur.<br><br>Ce guide doit : |

| | |
|---|---|
| | pas des fonctions d'administrateurs du système-cible ;<br>- Décrire l'utilisation des fonctions de sécurité fournies par le système-cible accessibles aux utilisateurs ;<br>- Contenir des avertissements concernant les fonctions et les privilèges accessibles aux utilisateurs qui devraient être contrôlés dans un environnement d'exploitation sûr ;<br>- Présenter clairement toutes les responsabilités qui incombent à l'utilisateur et qui sont nécessaires pour une exploitation sûre du système-cible, y compris celles liées aux hypothèses relatives au comportement de l'utilisateur figurant dans l'énoncé de l'environnement de sécurité du système-cible ;<br>- Être cohérent avec toute autre documentation fournie pour l'évaluation ;<br>- Décrire toutes les exigences de sécurité pour l'environnement TI, qui concernent l'utilisateur. |
| **EA.NUM-VERSION** | |
| Description | Le cabinet d'études doit disposer d'une référence unique (ou équivalent, numéro de version par exemple) de chaque version des entités du système-cible. Cette référence les identifie. |
| **EA.PROC-INSTALL** | |
| Description | Le cabinet d'études doit disposer d'une documentation décrivant les étapes nécessaires à une installation, une génération et un démarrage sûrs du système-cible. |
| **EA.SPECIFICATIONS** | |
| Description | Le cabinet d'études doit disposer des spécifications fonctionnelles informelles, cohérentes et complètes, des fonctions de sécurité du système-cible et de ses interfaces externes (dont il sera détaillé le but, le mode d'emploi, et si approprié les effets, exceptions et messages d'erreur). |
| **EA.TESTS** | |
| Description | Le système-cible doit pouvoir faire l'objet de tests indépendants de conformité (confirmation par un tiers que les informations fournies satisfont à toutes les exigences relatives au contenu et à la présentation des éléments de preuve, confirmation que le système-cible fonctionne conformément à ses spécifications). |

### 7.2.2 Dépendances des exigences d'assurance

Il est nécessaire de vérifier que l'ensemble des composants d'assurance retenu est "consistant". Or, ces composants sont ceux définis pour le niveau d'assurance EAL 1 dans l'ISO/IEC 15408. Ils sont donc parfaitement "consistants".

# 8 Conclusion

L'étude de sécurité du cabinet d'architecture a permis de déterminer un ensemble d'exigences de sécurité tout en formalisant et uniformisant les idées des différents acteurs.

Il a donc été possible de :

- garantir une vision globale et cohérente de la sécurité, qui est parfaitement adaptée au contexte de l'organisme ;

- fournir un vocabulaire et des concepts communs aux différents acteurs ;

- améliorer grandement la sensibilisation des utilisateurs ;

- analyser le système et ses enjeux, les besoins de sécurité des éléments essentiels, les menaces et les risques pesant sur l'organisme, les objectifs et exigences de sécurité permettant de s'en prémunir ;

- mettre en évidence les risques résiduels acceptés par l'organisme.

Une fois validée, cette étude menée à l'aide de la méthode EBIOS permettra la rédaction d'une FEROS (Fiche Rationnelle des Objectifs de Sécurité) ou de toute autre forme de cahier des charges de sécurité (notamment sous la forme ISO/IEC 15408 – Critères Communs, comme les profils de protection et cibles de sécurité) et constituera une base fondamentale pour l'élaboration d'un schéma directeur SSI, d'une PSSI (politique de sécurité des systèmes d'information) ou d'un tableau de bord SSI.

# Formulaire de recueil de commentaires

Ce formulaire peut être envoyé à l'adresse suivante :

Secrétariat général de la défense nationale
Direction centrale de la sécurité des systèmes d'information
Sous-direction des opérations
Bureau conseil
51 boulevard de La Tour-Maubourg
75700 PARIS 07 SP
conseil.dcssi@sgdn.pm.gouv.fr

**Identification de la contribution**
Nom et organisme (facultatif) : .....
Adresse électronique : .....
Date : .....

**Remarques générales sur le document**
Le document répond-il à vos besoins ? Oui ☐ Non ☐

Si oui :

Pensez-vous qu'il puisse être amélioré dans son fond ? Oui ☐ Non ☐

Si oui :

Qu'auriez-vous souhaité y trouver d'autre ?
.....
.....

Quelles parties du document vous paraissent-elles inutiles ou mal adaptées ?
.....
.....

Pensez-vous qu'il puisse être amélioré dans sa forme ? Oui ☐ Non ☐

Si oui :

Dans quel domaine peut-on l'améliorer ?
- lisibilité, compréhension ☐
- présentation ☐
- autre ☐

Précisez vos souhaits quant à la forme :
.....
.....

Si non :

Précisez le domaine pour lequel il ne vous convient pas et définissez ce qui vous aurait convenu :
.....
.....

Quels autres sujets souhaiteriez-vous voir traiter ?
.....
.....

**Remarques particulières sur le document**

Des commentaires détaillés peuvent être formulés à l'aide du tableau suivant.

"N°" indique un numéro d'ordre.

"Type" est composé de deux lettres :

La première lettre précise la catégorie de remarque :

- O Faute d'orthographe ou de grammaire
- E Manque d'explications ou de clarification d'un point existant
- I Texte incomplet ou manquant
- R Erreur

La seconde lettre précise son caractère :

- m mineur
- M Majeur

"Référence" indique la localisation précise dans le texte (numéro de paragraphe, ligne…).

"Énoncé de la remarque" permet de formaliser le commentaire.

"Solution proposée" permet de soumettre le moyen de résoudre le problème énoncé.

| N° | Type | Référence | Énoncé de la remarque | Solution proposée |
|---|---|---|---|---|
| 1 | | | | |
| 2 | | | | |
| 3 | | | | |
| 4 | | | | |
| 5 | | | | |

Merci de votre contribution