XXXX

FEROS

Référence :

Date :

Version :

Etat : Projet

Diffusion : Diffusion restreinte

**Validation**

| Nom | Fonction | Signature |
| --- | --- | --- |
|  |  |  |
|  |  |  |

**Approbation**

| Nom | Fonction | Signature |
| --- | --- | --- |
|  |  |  |

|  |
| --- |
| Révisions |

| Version | Date | Objet | Auteurs |
| --- | --- | --- | --- |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

|  |
| --- |
| Sommaire |

[1 Introduction 5](#_Toc491087055)

[1.1 Objet du document 5](#_Toc491087056)

[1.2 Contexte général 5](#_Toc491087057)

[1.3 Définition des responsabilités 5](#_Toc491087058)

[2 Référentiel documentaire 6](#_Toc491087059)

[3 Glossaire 7](#_Toc491087060)

[4 Contexte de l’analyse de risques 8](#_Toc491087061)

[4.1 Périmètre de l’analyse de risques 8](#_Toc491087062)

[4.1.1 Organisation de la sécurité du système d’information de XXXX 8](#_Toc491087063)

[4.1.2 Rappel historique 8](#_Toc491087064)

[4.1.3 Périmètre et évolution 8](#_Toc491087065)

[4.1.4 Cadre règlementaire 8](#_Toc491087066)

[4.2 Enjeux de l’analyse 8](#_Toc491087067)

[5 Métriques utilisés 9](#_Toc491087068)

[5.1 Les critères de sécurité 9](#_Toc491087069)

[5.2 Echelle décisionnelle pour le traitement des risques 11](#_Toc491087070)

[5.2.1 Niveaux de risques 11](#_Toc491087071)

[5.2.2 Objectif de traitement des risques 11](#_Toc491087072)

[5.2.3 Plan de traitement 11](#_Toc491087073)

[6 Description du système 12](#_Toc491087074)

[6.1 Architecture fonctionnelle du Système 12](#_Toc491087075)

[6.2 Biens Essentiels 12](#_Toc491087076)

[6.3 Besoins de sécurité 12](#_Toc491087077)

[6.4 Biens Supports 14](#_Toc491087078)

[6.5 Relations entre biens essentiels et biens support 15](#_Toc491087079)

[7 Mesures de sécurité existantes 16](#_Toc491087080)

[8 Les sources de menaces 18](#_Toc491087081)

[9 Etude des événements redoutés 19](#_Toc491087082)

[10 Etude des scénarios de menaces 20](#_Toc491087083)

[11 Etude des risques 25](#_Toc491087084)

[11.1 Risques SSI identifiés 25](#_Toc491087085)

[11.2 Hiérarchisation des risques actuels 33](#_Toc491087086)

[11.3 Identification des objectifs SSI 34](#_Toc491087087)

[11.4 Méthodes d’attaques non retenues 34](#_Toc491087088)

[12 Etude des mesures de sécurité 35](#_Toc491087089)

[12.1 Mesures de sécurité nécessaires 35](#_Toc491087090)

[12.2 Risques résiduels 38](#_Toc491087091)

# Introduction

## Objet du document

L’objet de ce document est d’analyser les risques (en termes de sécurité de l’information) pesant sur les systèmes relatifs au ………….

Ce document porte le nom de « FEROS - XXX » et permet d’évaluer de façon qualitative les risques pesant sur les données à caractère personnel et les données sensibles.

## Contexte général

Le projet XXXX s’inscrit dans un contexte particulier, Méthodologie

La méthodologie retenue dans cette démarche d’analyse de risques repose sur cinq grandes phases et dérive principalement de la méthode Expression des Besoins et Identification des Objectifs de Sécurité (EBIOS) 2010, méthode définie par l’ANSSI :

1. Etude du contexte - Identification des biens essentiels et biens supports
2. Etude des événements redoutés
3. Etude des scénarios de menaces
4. Etude des risques
5. Etude des mesures sécurité

Cette méthodologie éprouvée permet une appréciation des risques de sécurité pesant sur ….

## Définition des responsabilités

L’analyse donnant lieu à ce document a été réalisée par ...

L’analyse de risques préliminaire s’est appuyée sur la méthode EBIOS développée par l’ANSSI.

# Référentiel documentaire

La présente FEROS est rédigée principalement à partir du référentiel documentaire suivant et complété avec les renseignements fournis par l’équipe gérant le projet.

| Référence | Titre du document | Version | Auteur | Date |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Glossaire

**ANSSI :** Agence Nationale de la Sécurité des Systèmes d’Information.

**EBIOS:** Expression des besoins et identification des objectifs de sécurité.

**FEROS:** Fiche d’Expression Rationnelle des Objectifs de Sécurité.

**SI :** Système d’Information

# Contexte de l’analyse de risques

## Périmètre de l’analyse de risques

Ce document présente l’analyse de risques de l’ensemble du système d’information.

### Organisation de la sécurité du système d’information de XXXX

Le schéma ci-dessous décrit la chaine fonctionnelle de la sécurité des systèmes d’information de XXXX :

### Rappel historique

La mise en place du système

.

### Périmètre et évolution

Le système, objet de ce document, concerne….

Le périmètre de l’analyse de risque se focalise sur ………………

### Cadre règlementaire

:

## Enjeux de l’analyse

Les changements ne doivent pas entrainer de baisse de sécurité du S.I. global de l’XXXX.

Les objectifs du Système…………. sont quant à eux multiples :

# Métriques utilisés

## Les critères de sécurité

Les critères de sécurité retenus sont la disponibilité, l’intégrité, la confidentialité et la traçabilité. Pour l’évaluation des risques, ce sont les échelles de gravité et de vraisemblance qui sont utilisées.

Les différentes échelles sont définies dans les tableaux suivants :

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | BESOIN DE SÉCURITÉ DES BIENS ESSENTIELS | | | |
|  | 1 | 2 | 3 | 4 |
| DISPONIBILITÉ | Le bien n’a pas un besoin particulier de disponibilité. | Rétablissement en moins d’un jour.  Une indisponibilité peut être tolérée avec un besoin de rétablissement dans un délai compris de 24h maximum, même en cas d’incident majeur. | Rétablissement dans les « 12h ».  Une indisponibilité peut être tolérée avec un besoin de rétablissement dans les 4 heures qui suivent. Même en cas d’incident majeur. | Haute disponibilité 24/24 et 7/7. |
| INTÉGRITÉ | Non contrôlé.  Pas de besoin d'intégrité particulier | Intègre.  Une perte momentanée d’intégrité est acceptée, si elle est corrigée dans un délai inférieur à 24h et ne remet pas en cause le service fourni. | Contrôle d’intégrité.  Une perte momentanée d'intégrité n'est pas acceptée.  Toute perte d'intégrité entraîne l'arrêt du service jusqu'au rétablissement de l'intégrité | Parfaitement intègre.  Aucune perte d’intégrité n’est acceptée.  Toute perte d’intégrité est corrigée immédiament sans impact sur le service. |
| CONFIDENTIALITÉ | Publique.  La connaissance de ces informations à l'intérieur ou l'extérieur ne présente aucun risque.  La connaissance de ces informations à l’intérieur ou l’extérieur ne présente aucun risque. | Restreint agent et utilisateur.  La divulgation de ces informations aux personnes non autorisées aurait des conséquences modérées. Elles ne doivent cependant pas être divulguées. | Diffusion restreinte  Informations soumises à l'obligation de réserve ou de discrétion professionnelle.  La divulgation de ces informations aux personnes non autorisées aurait des conséquences modérées. | Confidentiel  ex : données nominatives au sens de la loi informatique et libertés, articles de sécurité, clé privée…  La divulgation de ces informations aux personnes non autorisées pourrait avoir des conséquences critiques. |
| TRAÇABILITÉ | Le bien n’a pas un besoin particulier de traçabilité. | Traces incluant actions dates et heures  Pas de besoin de caractère probant, conséquences limitées en cas d'altération de ces traces. Mise à disposition dans un délai à posteriori. | Preuve interne – Traces incluant auteur, actions dates et heure  Elément de preuve des opérations immédiatement disponibles. Auditable dans une optique d’usage interne des moyens de preuve | Trace pouvant servir de preuve  Non-répudiation de l’opération effectuée. Niveau de preuve opposable dans un tribunal sur les événements système ou applicatif. |

Le tableau suivant représente l’échelle de gravité utilisée dans la suite du document :

|  |  |  |
| --- | --- | --- |
| **GRAVITE** | | |
| **Niveaux** | **Echelle des besoins** | **Description** |
| 1 | **Faible** | La solution surmontera les impacts sans aucune difficulté |
| 2 | **Limitée** | La solution surmontera les impacts malgré quelques difficultés |
| 3 | **Importante** | La solution surmontera les impacts avec de sérieuses difficultés |
| 4 | **Critique** | La solution ne surmontera pas les impacts |

Le tableau suivant représente l’échelle de vraisemblance utilisée dans la suite du document :

|  |  |  |
| --- | --- | --- |
| **VRAISEMBLANCE** | | |
| **Niveaux** | **Echelle des besoins** | **Description** |
| 1 | **Minime** | Cela ne se produira probablement jamais |
| 2 | **Significative** | La probabilité pour que cela se produise n'est pas nulle |
| 3 | **Forte** | Cela devrait se produire un jour ou l'autre |
| 4 | **Maximale** | Cela va certainement se produire prochainement et assez souvent |

## Echelle décisionnelle pour le traitement des risques

### Niveaux de risques

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Echelle de niveau du risque | | | | | |
| Gravité | 4 – Critique | 2 - Significatif | 2 - Significatif | 3 - Intolérable | 3 - Intolérable |
| 3 – Importante | 1 - Négligeable | 2 - Significatif | 2 - Significatif | 3 - Intolérable |
| 2 – Limitée | 1 - Négligeable | 1 - Négligeable | 2 - Significatif | 2 – Significatif |
| 1 – Faible | 1 - Négligeable | 1 - Négligeable | 1 - Négligeable | 2 – Significatif |
|  |  | 1 – Minime | 2 – Significative | 3 – Forte | 4 – Maximale |
|  |  | Vraisemblance | | | |

Pour la gestion des risques, trois niveaux de risques sont définis :

* Les risques dont la gravité est faible et la vraisemblance minime, significative ou forte, ainsi que les risques dont la gravité est limitée et la vraisemblance minime ou significative et les risques dont la gravité est importante et la vraisemblance est minime sont classés comme « **négligeables** »;
* Les risques dont la gravité est faible et la vraisemblance maximale, ceux dont la gravité est limitée et la vraisemblance est forte ou maximale, ceux dont la gravité est importante et de vraisemblance significative ou forte, et ceux dont la gravité est critique et la vraisemblance est minime sont classés « **significatifs** » ;
* Les risques dont la gravité est importante et la vraisemblance est maximale ou ceux dont la gravité est critique et la vraisemblance forte ou maximale sont jugés comme **« intolérables ».**

### Objectif de traitement des risques

L’objectif de traitement des risques est de ne plus avoir de risque « intolérable ». Le but est de limiter les risques résiduels à un niveau « significatif ».

### Plan de traitement

Les règles concernant le traitement des risques sont les suivantes :

* Les **risques intolérables** doivent être communiqués à …………………et être traités dans un délai inférieur à trois mois (réduction, transfert, évitement, prise). Les actions prévues doivent être décidées avant toute mise en production du service, sinon dans les meilleurs délais après qualification. Une dérogation de ……………… doit être obtenue si certaines actions ne sont pas prévues à la date de mise en production du service ;
* Les **risques significatifs** peuvent être tolérés dans le cadre de l’homologation du système par la ……………. Mais devront être traités avant l’évaluation ;
* Les **risques négligeables** peuvent être conservés mais doivent faire l’objet d’une réévaluation régulière.

# Description du système

## Architecture fonctionnelle du Système

XX

## Biens Essentiels

Les processus essentiels considérés dans la présente FEROS, en cohérence avec la description fonctionnelle du système-cible, sont les suivants :

| **Processus et référentiels essentiels** | **Description** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

## Besoins de sécurité

| **Biens essentiels** | **D** | **I** | **C** | **T** |
| --- | --- | --- | --- | --- |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

## Biens Supports

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | | | | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  | | | | |
|  | | | | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  | | | | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  | | | | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  |  |  |  | |
|  | | | | |
|  |  |  | |  |
|  | | | | |
|  |  |  |  | |

## Relations entre biens essentiels et biens support

| **Processus et référentiels essentiels** | **Biens support impactés** |
| --- | --- |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |
|  |  |

# Mesures de sécurité existantes

Le tableau suivant regroupe les mesures techniques ou organisationnelles existantes, pour traiter les risques identifiés initialement. L’objectif est de traiter ces risques au regard des objectifs de sécurité. Les mesures prises en compte dans le cadre de la présente analyse sont :

|  |  |  |
| --- | --- | --- |
| Mesures ISO27002 | | Contexte d’application |
| 6.1.5 | La sécurité de l’information dans la gestion de projet |  |
| 12.1.2 | Gestion des changements |
| 12.13 | Dimensionnement |
| 8.1.1 | Inventaire des actifs |  |
| 9.1.1 | Politique de contrôle d’accès |  |
| 9.1.2 | Accès aux réseaux et aux services réseau |
| 9.4.1 | Restriction d'accès à l'information |
| 9.4.2 | Sécuriser les procédures de connexion |
| 9.4.4 | Utilisation de programmes utilitaires à privilèges |
| 10.1.1 | Politique d'utilisation des mesures cryptographiques |  |
| 10.1.2 | Gestion des clés |
| 11.1.1 | Périmètre de sécurité physique |  |
| 11.1.2 | Contrôle d’accès physique |
| 11.1.4 | Protection contre les menaces extérieures et environnementales |
| 11.1.5 | Travail dans les zones sécurisées |
| 11.2.1 | Emplacement et protection des matériels |
| 11.2.3 | Sécurité du câblage |
| 11.2.4 | Maintenance des matériels |
| 11.2.5 | Sortie des actifs |
| 12.2.1 | Mesures contre les logiciels malveillants |  |
| 12.3.1 | Sauvegarde des informations |  |
| 12.4.1 | Journalisation des événements |  |
| 12.4.2 | Protection de l’information journalisée |
| 12.4.3 | Journaux administrateur et opérateur |
| 12.4.4 | Synchronisation des horloges |
| 13.1.1 | Contrôle des réseaux |  |
| 13.1.2 | Sécurité des services de réseaux |
| 13.1.3 | Cloisonnement des réseaux |
| 13.2.1 | Politiques et procédures de transfert de l'information |
| 14.1.1 | Analyse et spécification des exigences de sécurité de l’information |  |
| 14.1.2 | Sécurisation des services d’application sur les réseaux publics |
| 14.1.3 | Protection des transactions liées aux services d’application |
| 14.2.1 | Politique de développement sécurisé |
| 14.2.5 | Principes d’ingénierie de la sécurité des systèmes |
| 15.1.1 | Politique de sécurité de l'information dans les relations avec les fournisseurs |  |
| 15.1.2 | La sécurité dans les accords conclus avec les fournisseurs |
| 15.1.3 | Chaîne d'approvisionnement des produits et des services informatiques |
| 16.1.7 | Collecte des preuves |  |
| 17.2.1 | Disponibilité des moyens de traitement de l’information |  |

# Les sources de menaces

Dans le cadre de la présente analyse, le tableau ci-dessous, liste l’ensemble des sources de menaces retenues souhaite s’opposer aux sources de menaces suivante :

| **Types de sources de menaces** | **S'y opposer : oui ou non** | **Exemple** |
| --- | --- | --- |
| **Sources Humaines** | | |
| Source humaine interne, malveillante, avec de faibles capacités | Oui | > Employé et/ou prestataire en fin de contrat voulant se venger.  > Personnel d'entretien. |
| Source humaine interne, malveillante, avec des capacités importantes | Oui | > Administrateur mécontent. > Sous-traitant (Développement). |
| Source humaine interne, malveillante, avec des capacités illimitées | Oui | > Administrateur système ou réseaux agissant par vengeance. |
| Source humaine externe, malveillante, avec de faibles capacités | Oui | > Script kiddies. |
| Source humaine externe, malveillante, avec des capacités importantes | Oui | > Pirate à travers Internet.  > Agence gouvernementale souhaitant recueillir des informations confidentielles.  > Groupe de hackers soutenus par un Etat étranger.  >Organisation terroriste. |
| Source humaine interne, sans intention de nuire, avec de faibles capacités | Oui | > Employé et/ou prestataire. |
| Source humaine interne, sans intention de nuire, avec des capacités importantes | Oui | > Développeur inexpérimenté. |
| Source humaine interne, sans intention de nuire, avec des capacités illimitées | Oui | > Administrateur système ou réseau. |
| Source humaine externe, sans intention de nuire, avec des capacités importantes | Oui | > Exploitant.  >Hébergeur. |
| **Sources non- humaines** | | |
| Code malveillant | Oui | > Virus ciblé ou pas.  > Ransomware. |

# Etude des événements redoutés

Le tableau ci-après liste les événements redoutés en termes de Disponibilité, d’Intégrité, de Confidentialité et de Traçabilité, pesant sur les biens essentiels.

En fonction de l’impact sur le SIV, l’événement redouté a un niveau de gravité différent.

Cette étude est menée en fonction des mesures de sécurité existantes.

| N° | Evénement redouté | Biens essentiels | Impacts | Besoin de sécurité | Gravité actuelle |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  | Disponibilité | Critique |
|  |  |  |  | Intégrité | Important |
|  |  |  |  | Confidentialité | Critique |
|  |  |  |  | Intégrité | Important |
|  |  |  |  | Disponibilité | **Limitée** |
|  |  |  |  | Intégrité  Traçabilité | Critique |
|  |  |  |  | Confidentialité | Critique |
|  |  |  |  | Confidentialité  Traçabilité | Important |
|  |  |  |  | Confidentialité | Important |

# Etude des scénarios de menaces

Ce chapitre présente la répartition des menaces pesant sur les biens supports en fonction de leur vraisemblance et leur impact sur la disponibilité, l’intégrité, la confidentialité et la traçabilité.

| SM n° | Scénario de menace | Bien support | D | I | C | T | Prérequis | Vraisemblance  initiale | Vraisemblance  actuelle |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| SM01 |  |  | X | X |  | X |  | 2 - Significative | 1 - Minime |
| SM02 |  |  | X |  |  |  |  | 3 - Forte | 2 - Significative |
| SM03 |  |  |  | X |  | X |  | 2 - Significative | 1 - Minime |
| SM04 |  |  |  |  | X |  |  | 3 - Forte | 2 - Significative |
| SM05 |  |  | X |  | X |  |  | 3 - Forte | 2 - Significative |
| SM06 |  |  |  | X |  | X |  | 3 - Forte | 2 - Significative |
| SM07 |  |  | X | X | X | X |  | 3 - Forte | 2 - Significative |
| SM08 |  |  | X | X |  |  |  | 3 - Forte | 2 - Significative |
| SM09 |  |  | X | X | X | X |  | 3 - Forte | 2 - Significative |
| SM10 |  |  | X | X |  |  |  | 2 - Significative | 1 - Minime |
| SM11 |  |  | X | X |  |  |  | 2 - Significative | 2 - Significative |
| SM12 |  |  |  |  | X | X |  | 4 - Maximale | 3 - Forte |
| SM13 |  |  | X | X | X | X |  | 2 - Significative | 1 - Minime |
| SM14 |  |  |  |  | X |  |  | 4 - Maximale | 3 - Forte |
| SM15 |  |  | X | X |  |  |  | 2 - Significative | 1 - Minime |
| SM16 |  |  |  |  |  | X |  | 3 - Forte | 2 - Significative |
| SM17 |  |  | X |  | X |  |  | 2 - Significative | 1 - Minime |
| SM18 |  |  | X |  |  |  |  | 3 - Forte | 2 - Significative |
| SM19 |  |  | X |  | X |  |  | 3 - Forte | 2 - Significative |
| SM20 |  |  |  |  | X |  |  | 4 - Maximale | 3 - Forte |
| SM22 |  |  |  |  | X | X |  | 3 - Forte | 2 - Significative |
| SM23 |  |  |  |  | X |  |  | 3 - Forte | 2 - Significative |
| SM24 |  |  |  |  | X | X |  | 3 - Forte | 2 - Significative |
| SM25 |  |  | X |  |  |  |  | 2 - Significative | 1 - Minime |
| SM26 |  |  |  |  | X | X |  | 4 - Maximale | 3 - Forte |
| SM27 |  |  |  | X |  |  |  | 4 - Maximale | 3 - Forte |
| SM28 |  |  |  |  | X |  |  | 4 - Maximale | 3 - Forte |
| SM29 |  |  | X | X |  |  |  | 2 - Significative | 1 - Minime |
| SM30 |  |  | X | X |  |  |  | 2 - Significative | 1 - Minime |
| SM31 |  |  |  |  | X |  |  | 3 - Forte | 2 - Significative |
| SM32 |  |  | X | X | X |  |  | 3 - Forte | 2 - Significative |
| SM33 |  |  |  | X |  |  |  | 4 - Maximale | 4 - Maximale |

# Etude des risques

## Risques SSI identifiés

|  |  |  |
| --- | --- | --- |
| **R01 : XXXXXXXXXXXXXXXXXXX** | | |
| *Description* |  | |
| *Scénarios de menaces* |  | **1 - Minime** |
|  | **2 - Significative** |
|  | **2 - Significative** |
|  | **2 - Significative** |
|  | **1 - Minime** |
|  |  |
|  |  |
|  |  |
|  |  |
| *Commentaire* | Défaut du Maintien en Condition de Sécurité | |
| Gravité actuelle | 5- Critique | |
| Vraisemblance | 2 - Significative | |

|  |  |  |
| --- | --- | --- |
| **Niveau de risque** | Initial | 3 - Intolérable |
| Actuel | 2 - Significatif |
| Cible | 1 - Négligeable |

|  |  |  |
| --- | --- | --- |
| **R02 : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXX.** | | |
| *Libellé* | Les données concernant les ……………ne sont pas cohérentes | |
| *Scénarios de menaces* |  | **1 - Minime** |
|  | **2 - Significative** |
|  |  |
|  | **1 - Minime** |
|  | **–3 - Forte** |
|  |  |
|  |  |
| *Commentaire* | Mauvaise prise en compte des mesures de sécurité dans les projets | |
| Gravité actuelle | 3 - Importante | |
| Vraisemblance | 3 - **Forte** | |

|  |  |  |
| --- | --- | --- |
| **Niveau de risque** | Initial | 3 - Intolérable |
| Actuel | 2 - Significatif |
| Cible | 1 - Négligeable |

|  |  |  |
| --- | --- | --- |
| R03 : XXXXXXXXXXXXXXXXXXXXXXXXXXXX | | |
|  |  | |
|  |  | **2 - Significative** |
|  | **2 - Significative** |
|  | **1 - Minime** |
|  | **–3 - Fort** |
|  | **1 - Minime** |
|  | 3 - Forte |
|  |  | 2 - Significative |
|  |  | 3 - Forte |
|  |  | 3 - Forte |
|  |  | 2 - Significative |
| *Commentaire* | Contrôles des habilitations inefficaces | |
| Gravité actuelle | 4 - Critique | |
| Vraisemblance | 3 - **Forte** | |

|  |  |  |
| --- | --- | --- |
| **Niveau de risque** | Initial | 3 - Intolérable |
| Actuel | 2 - Significatif |
| Cible | 1 - Négligeable |

|  |  |  |
| --- | --- | --- |
| **R04 : XXXXXXXXXXXXXXXXXXXXX** | | |
|  |  | |
|  |  | **1 - Minime** |
|  | **2 - Significative** |
|  | **2 - Significative** |
|  | **1 - Minime** |
|  | **1 - Minime** |
|  |  | **3 - Fort** |
| *Commentaire* | Instructions imprécises données à un sous-traitant | |
| Gravité actuelle | 3 - Importante | |
| Vraisemblance | 3 - Forte | |

|  |  |  |
| --- | --- | --- |
| **Niveau de risque** | Initial | 3 - Intolérable |
| Actuel | 2 - Significatif |
| Cible | 1 - Négligeable |

|  |  |  |
| --- | --- | --- |
| R05 : XXXXXXXXXXXXXXXXXXXXXXX | | |
|  |  | |
|  |  | **2 - Significative** |
|  | **2 - Significative** |
|  | **2 - Significative** |
|  |  | **1 - Minime** |
|  |  | **1 - Minime** |
|  |  | **1 - Minime** |
|  |  | **2 - Significative** |
|  |  | **3 - Fort** |
|  |  | **1 - Minime** |
|  |  |  |
| *Commentaire* | Mauvaise gestion d’un incident de sécurité | |
| Gravité actuelle | 1 - Limitée | |
| Vraisemblance | – 3 - Fort | |

|  |  |  |
| --- | --- | --- |
| **Niveau de risque** | Initial | 3 - Intolérable |
| Actuel | 2 - Significatif |
| Cible | 1 - Négligeable |

|  |  |  |
| --- | --- | --- |
| **R06 : XXXXXXXXXXXXXXXXXXXXXXXXxx** | | |
| *Libellé* |  | |
|  |  | **1 - Minime** |
|  | **2 - Significatif** |
|  | **4 -**  **Maximale** |
| *Commentaire* | Mauvaise maitrise des actifs | |
| Gravité actuelle | 4 - Critique | |
| Vraisemblance | 4 - Maximale | |

|  |  |  |
| --- | --- | --- |
| **Niveau de risque** | Initial | 3 - Intolérable |
| Actuel | 2 - Significatif |
| Cible | 1 - Négligeable |

R07 : XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

|  |  |  |
| --- | --- | --- |
|  |  | |
|  |  | **2 - Significative** |
|  | **3 - Forte** |
|  |  | **3 - Forte** |
| *Commentaire* | Procédure de Gestion des incidents inefficace | |
| Gravité actuelle | 4 - Critique | |
| Vraisemblance | 3- Forte | |

|  |  |  |
| --- | --- | --- |
| **Niveau de risque** | Initial | 3 - Intolérable |
| Actuel | 2 - Significatif |
| Cible | 1 - Négligeable |

|  |  |  |
| --- | --- | --- |
| **R08:XXXXXXXXXXXXXXXXXXXXXXXXXXXXX** | | |
| *Libellé* |  | |
| *Scénarios de menaces* |  | **2 - Significative** |
|  | **2 - Significative** |
|  | **2 - Significative** |
|  |  |
| *Commentaire* | Absence de contrôle chez les sous-traitants | |
| Gravité actuelle | 3 - Importante | |
| Vraisemblance | **2 - Significative** | |

|  |  |  |
| --- | --- | --- |
| **Niveau de risque** | Initial | 3 - Intolérable |
| Actuel | 2 - Significatif |
| Cible | 1 - Négligeable |

|  |  |  |
| --- | --- | --- |
| **R09: XXXXXXXXXXXXXXXXXXXXXXXXXXXXX** | | |
| *Libellé* |  | |
|  |  | **2 - Significative** |
|  | **2 - Significative** |
|  | **2 - Significative** |
| *Commentaire* |  | |
| Gravité actuelle | 3 - Importante | |
| Vraisemblance | 2 - Significatif | |

|  |  |  |
| --- | --- | --- |
| **Niveau de risque** | Initial | 3 - Intolérable |
| Actuel | 2 - Significatif |
| Cible | 1 - Négligeable |

## Hiérarchisation des risques actuels

Le tableau suivant détaille les risques identifiés et les classe en fonction de leur gravité et de leur vraisemblance.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Echelle de niveau du risque | | | | | |
| Gravité | 4 – Critique |  | R01, | R03, R07 | R06 |
| 3 – Importante |  | R08, R09 | R02, R04 |  |
| 2 – Limitée |  |  |  |  |
| 1 – Faible |  |  | R05 |  |
|  |  | 1 – Minime | 2 – Significative | 3 – Forte | 4 – Maximale |
|  |  | Vraisemblance | | | |

|  |
| --- |
| **R01 :** |
| **R02 :** |
| **R03 :** |
| **R04 :** |
| **R05 :** |
| **R06 :** |
| **R07:** |
| **R08:** |
| **R09:** |

## Identification des objectifs SSI

Cette activité fait partie du traitement des risques. Elle a pour but de choisir la manière dont chaque risque doit être traité au regard de son évaluation. Au regard des risques identifiés, les objectifs de sécurité identifiés dans le cadre du projet doivent permettre de garantir :

* Le bon fonctionnement du Système
* La confiance des usagers
* La protection des données sensibles du Système
* La lutte contre la fraude
* La conformité réglementaire

Le tableau ci-après présente le choix des objectifs de sécurité. Un objectif correspond au choix d’une des options listées ci-après :

* Eviter le risques : Changer le contexte de telle sorte que XXXX n'y soit plus exposée ;
* Réduire le risque : XXXX met en œuvre des mesures de sécurité pour diminuer la gravité et/ou la vraisemblance ;
* Prendre le risque : XXXX assume les conséquences sans prendre de mesure de sécurité particulière;
* Transférer le risque : XXXX partage les pertes occasionnées par un sinistre ou fait assumer la responsabilité à un (des) tiers.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Risques** | **Accepté** | **Evité** | **Réduction** | **Transfert** |
| R01 : |  |  | X |  |
|  |  |  | X |  |
|  |  |  | X |  |
|  |  |  | X |  |
|  |  |  | X |  |
|  |  |  | X |  |
|  |  |  | X |  |
|  |  |  | X |  |
|  |  |  | X |  |

## Méthodes d’attaques non retenues

Les scénarios de menace reposant sur des sinistres environnementaux ou locaux aux sites d’exploitation ne sont pas considérés dans le cadre de ce document.

Les scénarios de menace relatifs à des scénarios de fraude ou des dysfonctionnements du système de production, ne sont pas non plus retenus dans le cadre de la présente FEROS.

# Etude des mesures de sécurité

## Mesures de sécurité nécessaires

Le tableau suivant propose des recommandations avec des mesures de sécurité techniques ou organisationnelles, pour traiter les risques au regard des objectifs de sécurité identifiés dans la partie 9.3 du présent document.

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectif ISO27002 : Mise en place d’un SMSI** | | | |
| **Référence** | Management de la sécurité de l’information | **Type de mesure** | ORG |
| Un système de management de la sécurité de l’information doit être mis en place afin de maintenir le système à un niveau de sécurité conforme aux besoins et aux exigences légales.. | | | |
| Principaux risques couverts : R01, R02, R03, R04, R05, R06, R07 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectif ISO27002-7 : Information, Sensibilisation, Formation** | | | |
| **Référence** | SENSIBILISATION | **Type de mesure** | ORG |
|  | | | |
| Principaux risques couverts : R02, R03, R04, R05, R06 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectif ISO27002-8 : Gestion des actifs** | | | |
| **Référence** | ACTIFS | **Type de mesure** | ORG |
|  | | | |
| Principaux risques couverts : R01, R02, R03, R04, R05, R06 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectif ISO27002-9 : Contrôle des accès** | | | |
| **Référence** | ACCES | **Type de mesure** | ORG |
| . | | | |
| Principaux risques couverts : R01, R02, R03, R04, R05, R06, R07 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectif ISO27002-12 : Maintien en Condition Sécurité** | | | |
| **Référence** | EXPLOITATION | **Type de mesure** | ORG/TECH |
|  | | | |
| Principaux risques couverts : R01, R02, R03, R04, R05, R06, R07 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectif ISO27002-14 : Ingénierie du développement** | | | |
| **Référence** | DEVELOPPEMENT | **Type de mesure** | TECH |
|  | | | |
| Principaux risques couverts : R01, R02, R03, R05, R06, R07 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectif ISO27002-15 : Relations fournisseurs** | | | |
| **Référence** | PRESTATION | **Type de mesure** | ORG |
|  | | | |
| Principaux risques couverts : R06, R07 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectif ISO27002-16 : Incidents de sécurité** | | | |
| **Référence** | INCIDENT | **Type de mesure** | ORG |
|  | | | |
| Principaux risques couverts : R01, R02, R03, R04, R05, R06 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectif ISO27002-17 : Plan de Continuité d’Activité** | | | |
| **Référence** | PCA | **Type de mesure** | ORG |
|  | | | |
| Principaux risques couverts : R01, R02 | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Objectif ISO27002-18 : Conformité** | | | |
| **Référence** | CONFORMITE | **Type de mesure** | ORG |
|  | | | |
| Principaux risques couverts : R06 | | | |

## Risques résiduels

Le tableau ci-après récapitule les risques résiduels pesant sur le SIV. Après application des mesures de sécurité identifiées précédemment, le niveau initial de chaque risque a été revu.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Echelle de niveau du risque | | | | | |
| Gravité | 4 – Critique |  |  |  |  |
| 3 – Importante | R03, R05  R02, R04, R06 |  |  |  |
| 2 – Limitée |  | R01, R07 |  |  |
| 1 – Faible |  |  |  |  |
|  |  | 1 – Minime | 2 – Significative | 3 – Forte | 4 – Maximale |
|  |  | Vraisemblance | | | |

|  |
| --- |
| **R01 :** |
| **R02 :** |
| **R03** |
| **R04 .** |
| **R05** |
| **R06 :** |
| **R07:** |

Pour la répartition, des risques résiduels, on peut notifier qu’il n’y a aucun risque de niveau intolérable, ni de risque significatif avec une vraisemblance maximale.

Il est recommandé d’accepter les risques résiduels en l’état.

|  |
| --- |
| Fin du document |