# EXTRAIT DU REGISTRE DES DELIBERATIONS DU CONSEIL MUNICIPAL

SEANCE DU **14 avril 2017 à 18 h 00**

**----------**

AUJOURD'HUI **quatorze avril deux mille dix sept**

**LE CONSEIL MUNICIPAL** de la Ville de Clermont-Ferrand, convoqué par Monsieur le Maire le 07 avril 2017, s'est réuni dans la salle ordinaire des séances.

Après avoir ouvert la séance, Monsieur le Maire procède à l'appel.

Etaient présents Mmes et MM. les Membres du Conseil dont les noms suivent :

**Olivier BIANCHI, Maire, présidant la séance**

| | |
|---|---|
| **Présent(e)s :** | **Olivier BIANCHI, Françoise NOUHEN, Christine DULAC-ROUGERIE, Monique BONNET, Manuela FERREIRA DE SOUSA, Philippe BOHELAY, Simon POURRET, Isabelle LAVEST, Grégory BERNARD, Cécile AUDET, Jérôme GODARD, Cyril CINEUX, Jérôme AUSLENDER, Nicaise JOSEPH, Marion CANALES, Saïd Akim BARA, Gérard BOHNER, Nicolas BONNET, Dominique ADENOT, Valérie BERNARD, Christophe BERTUCAT, Jean-Luc BLANC, Dominique BRIAT, Edith CANDELIER, Jean-Christophe CERVANTES, Alparslan COSKUN, Louis COUSTÈS, Sondès EL HAFIDHI, Magali GALLAIS, Patricia GUILHOT, Pascal GUITTARD, Christiane JALICON, Claudine KHATCHADOURIAN-TECER, Alain LAFFONT, Pierre MIQUEL, Didier MULLER, Florent NARANJO, Nicole PRIEUX, Dominique ROGUE-SALLARD, Sylviane TARDIEU, Odile VIGNAL, Guillaume VIMONT** |
| **Excusé(e)s ayant donné pouvoir :** | **Jean-Pierre BRENAS à Edith CANDELIER, Nadia GUERMIT-MAFFRE à Jean-Luc BLANC, Jean-Pierre LAVIGNE à Louis COUSTÈS, Marianne MAXIMI à Florent NARANJO, Abdelmajid MELLOUKI à Cécile AUDET, Fabienne MONTEL à Christiane JALICON, Christian PORTEFAIX à Philippe BOHELAY, Laurence SCHLIENGER à Patricia GUILHOT** |
| **Excusé(e)s :** | **François BARRIÈRE, Géraldine BASTIEN** |
| **Absent(e)s** : | **Anne FAUROT, Isabelle PADOVANI, Antoine RECHAGNEUX** |
| **Secrétaire** : | **Guillaume VIMONT** |

***Monsieur le Maire, après avoir fait l'appel interrompt la séance à 18 h 19 pour recevoir, avec les présidents de groupe, une délégation du personnel des Galeries Lafayette.***
***Madame Sondès EL HAFIDHI arrive pendant la suspension de séance.***
***Le quorum étant atteint, Monsieur le Maire reprend la séance à 18 h 53.***
***Madame Françoise NOUHEN quitte la séance pendant les questions 3 et 4.***
***Monsieur Louis COUSTES part avant le vote de la question 3 sans laisser de pouvoir (fin du pouvoir de M. Jean-Pierre LAVIGNE).***
***Monsieur Alain LAFFONT quitte la séance avant le vote de la question 7 et donne pouvoir à Monsieur Alparslan COSKUN.***
***Madame Christine DULAC-ROUGERIE part avant le vote de la question 8 et laisse pouvoir à Madame Manuela FERREIRA DE SOUSA.***
***Madame Isabelle LAVEST et Monsieur Grégory BERNARD partent sans laisser de pouvoir avant le vote du vœu.***

---

**Rapport N° 13**

# HOMOLOGATION DE TÉLÉ-SERVICES MIS EN OEUVRE AU SEIN DE LA VILLE DE CLERMONT-FERRAND

---

L'utilisation courante de l'outil informatique et les relations dématérialisées avec les usagers et les autres administrations, nécessitent un climat de confiance entre tous les acteurs. La Commune utilise au quotidien l'outil informatique et numérique mais offre aussi à ses administrés, ses partenaires et fournisseurs des services en ligne et des services dématérialisés qui, avec l'évolution technologique et les avancées en termes de service à la population, vont être amenés à se développer.

La réglementation impose aux communes de mettre en œuvre le Référentiel Général de Sécurité (RGS) créé par l'article 9 de l'ordonnance du 8 décembre 2005, modifiée. Ce référentiel vise à mettre en place de bonnes pratiques de gestion de la sécurité des télé-services.
Par télé-services, il faut entendre, tous les échanges électroniques entre les administrations et les usagers ainsi que les échanges électroniques entre les administrations elles-mêmes courrier électronique, transferts de données via une application, échanges d'information sur un site internet.

L'homologation est formalisée par un document qui atteste de la conformité d'une application ou d'un télé-service aux règles définies par le Référentiel général de sécurité (RGS).
Le référentiel général de sécurité fixe les règles auxquelles les systèmes d'information mis en place par les autorités administratives doivent se conformer pour assurer la sécurité des informations échangées, et notamment leur confidentialité et leur intégrité, ainsi que la disponibilité et l'intégrité de ces systèmes et l'identification de leurs utilisateurs.

Les principaux acteurs de l'homologation sont :

- L'autorité d'homologation
L'autorité d'homologation est la personne physique qui, après instruction du dossier d'homologation, prononce l'homologation de sécurité du système d'information, c'est-à-dire prend la décision d'accepter les risques résiduels identifiés sur le système.
L'autorité d'homologation doit être désignée à un niveau hiérarchique suffisant pour assumer toutes les responsabilités, y compris éventuellement pénale, afférentes à cette décision d'homologation.

- La commission d'homologation
La commission d'homologation assiste l'autorité d'homologation pour l'instruction de l'homologation et est chargée de préparer la décision d'homologation.
La taille et la composition de cette commission doivent être adaptées à la nature du système et proportionnées à ses enjeux. Cette commission, réunit les responsables métier concernés par le service à homologuer et des experts techniques.

La Ville de Clermont-Ferrand,

Vu l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives,

Vu, le décret n° 2010-112 du 2 février 2010 pris pour l'application des articles 9, 10 et 12 de l'ordonnance n° 2005-1516 du 8 décembre 2005 relative aux échanges électroniques entre les usagers et les autorités administratives et entre les autorités administratives.

Vu l'arrêté du 13 juin 2014 portant approbation du référentiel général de sécurité version 2,0 et précisant les modalités de mise en œuvre de la procédure de validation des certificats électroniques et sa version consolidée du 1er juillet 2014,

Vu la circulaire de l'Agence Nationale de la Sécurité des Systèmes d'Information du 3 novembre 2014 et son annexe ;

Considérant qu'il revient au Conseil de nommer l'autorité d'homologation qui sera habilitée à homologuer les télé-services de la Ville ;

Considérant qu'une commission d'homologation, chargée d'assister l'autorité d'homologation, doit être créée pour examiner les dossiers constitués en vue de l'homologation des systèmes d'information ;

Considérant que l'homologation doit intervenir selon le protocole joint en annexe (cf annexe sur CD),

Il vous est proposé :

- de décider à l'unanimité de procéder à la désignation de l'autorité d'homologation pour la Ville de Clermont- Ferrand selon la possibilité offerte par les dispositions de l'article L2121-21 du Code Général des Collectivités Territoriales ;

- de désigner Monsieur Jérôme AUSLENDER, Adjoint en charge de l'Enseignement Supérieur, la recherche, la Vie Étudiante et les Relations Internationales, comme autorité d'homologation pour la Ville de Clermont-Ferrand, autorité qui sera désormais chargé de délivrer une attestation d'homologation pour les télé-services de la Ville ;

- de créer une Commission d'homologation, qui assistera l'autorité d'homologation dans sa tâche et composée du Directeur, du responsable Sécurité du Systèmes d'Information, du responsable Correspondant Informatique et Libertés, les Responsables Projets Fonctionnels, le responsable du Service Infrastructure, le responsable du service Applications et Usages Métiers ;

– de valider le processus d'homologation tel que définit dans l'annexe 1(cf annexe sur CD).

## DELIBERATION

Le principe du vote à main levée est adopté à l'unanimité. Les propositions misent aux voix sont adoptées à la majorité et convertie en délibération.

Pour ampliation certifiée conforme.

Fait à Clermont-Ferrand, le 2 mai 2017

Pour le Maire et par délégation
L'Adjoint au Maire,
Jérôme Auslender

**Annexe N°1 de la délibération n° du 14/04/2017**



Mairie de Clermont-Ferrand,

Homologation des télé-services

14/04/2017

## Homologation Des Télé-services

Les télé-services de la Mairie portent sur 3 familles :

- Un groupe de télé-services sans authentification qui porte sur des formulaires d'état civil ou autres type de demande, dans lesquels l'usager déposes des données très peu confidentielles. Ces télé-services sont accessibles depuis Internet ou depuis une application mobile.
- 2 télé-services avec authentification (kiosque famille et Concessions funéraires), accessibles depuis l'Internet, avec un niveau de confidentialité des données supérieur.
- Un télé-service d'accès à des applications par des partenaires accessible depuis l'Internet et pour lequel le niveau de confidentialité dépend de l'application accédée.

© Sogeti

## Homologation Des Télé-services

L'homologation, c'est quoi ?

- Comme tout télé-service, ceux de la Mairie de Clermont-Ferrand sont soumis au RGS (*) issu de la loi de confiance dans l'économie numérique, et doivent donc être homologués.
- L'homologation est prononcée en interne par une autorité.
- Le processus d'homologation qui a été mis en place respecte les directives décrites dans le guide d'homologation de l'ANSSI (**)
- La commission d'homologation a été constituée conformément à la stratégie d'homologation de la Mairie de Clermont-Ferrand. Elle a pour mission de donner un avis motivé à l'autorité d'homologation qui doit statuer sur la mise en service.
- Le dossier d'homologation, que le présent document décrit, est remis à l'ensemble des membres de la commission d'homologation pour analyse avant la réunion finale de décision.

(*) Référentiel Général de sécurité
(**) Agence Nationale de Sécurité des Systèmes d'Information

© Sogeti 

## Composition de la commission d'homologation

Conformément à la stratégie d'homologation de la Mairie de Clermont-Ferrand, la commission d'homologation des télé-services est composée des personnes suivantes :

- Mr BOST : Directeur de la DSIT, RSSI et CIL;
- Mme ESSABIR : Responsable projet fonctionnel du kiosque;
- Mme GARDET : Responsable projet fonctionnel « funéraire »;
- Mr HOUE: Responsable pôle systèmes d'information progiciel ;
- Mr ANDREJEWSKI : Responsable pôle développement ;
- Mr AMADELLI : Responsable infrastructure;

© Sogeti 

## Détermination de la démarche requise

Sur la base du questionnaire d'auto-évaluation issu du guide d'homologation de l'ANSSI, réalisé avec Mr HOUE, Mr DIJOUX, Mr AMADELLI, Mr GHIBAUDO, Mr SAULNIER, ont été identifiés :

- Les processus et fonctions des télé-services.
- Les données traitées et leur criticité.
- Le niveau de démarche RGS requis.

Le choix de niveau de la démarche a été déterminé sur la base du guide d'homologation ANSSI qui détermine les pièces constitutives du dossier d'homologation qui vous a été remis le 01/12/2016

© Sogeti 

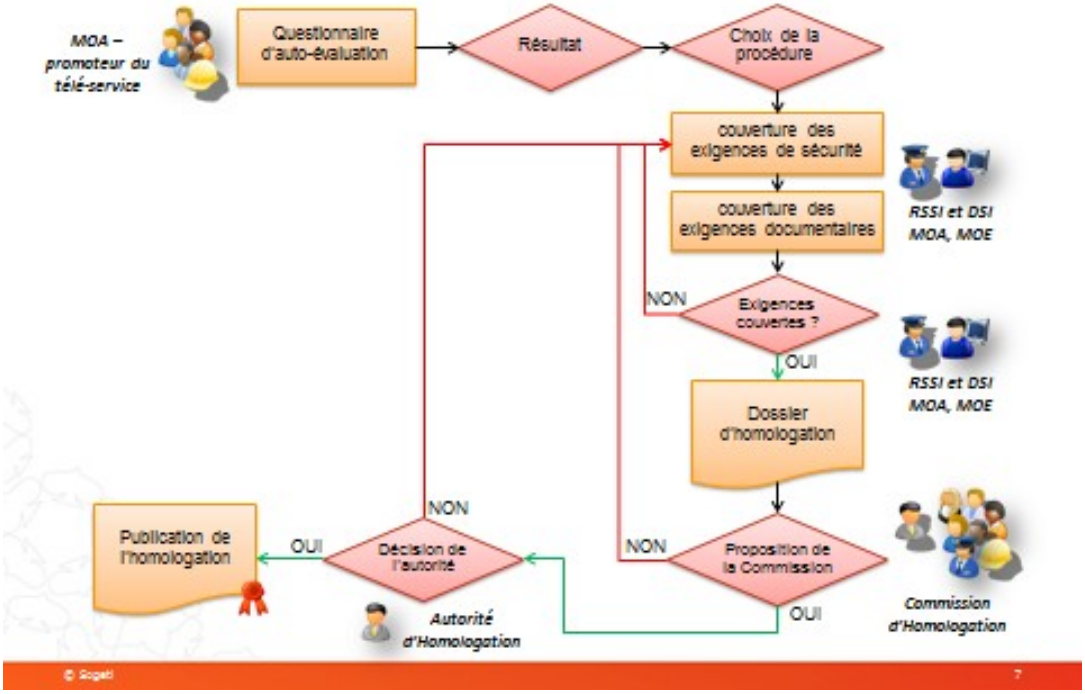
## Résultats de l'auto-évaluation

| | |
|---|---|
| Synthèse du besoin en sécurité | Moyen |
| Synthèse du niveau de maturité | Elémentaire |
| Type de procédure préconisée ==> | Mezzo-Forte |

| Quels documents pour constituer le dossier d'homologation selon la procédure retenue ? | |
|---|---|
| **Document** | **Besoin** |
| Stratégie d'homologation | Indispensable |
| Référentiel de sécurité | Si existant |
| Risques identifiés et objectifs de sécurité | Indispensable |
| Politique de sécurité des systèmes d'information | Recommandé |
| Procédures d'exploitation sécurisée du système | Indispensable |
| Journal de bord de l'homologation | Recommandé |
| Certificats de qualification des produits ou prestataires | Si existant |
| Résultats d'audits | Si existant |
| Liste des risques résiduels | Indispensable |
| Décision d'homologation | Indispensable |
| **S'agit-il d'un télé-service déjà en fonction ?** | **Oui** |
| Tableau de bord des incidents et de leur résolution | Recommandé |
| Résultats d'audits intermédiaires | Si existant |
| Journal des évolutions du système | Si existant |

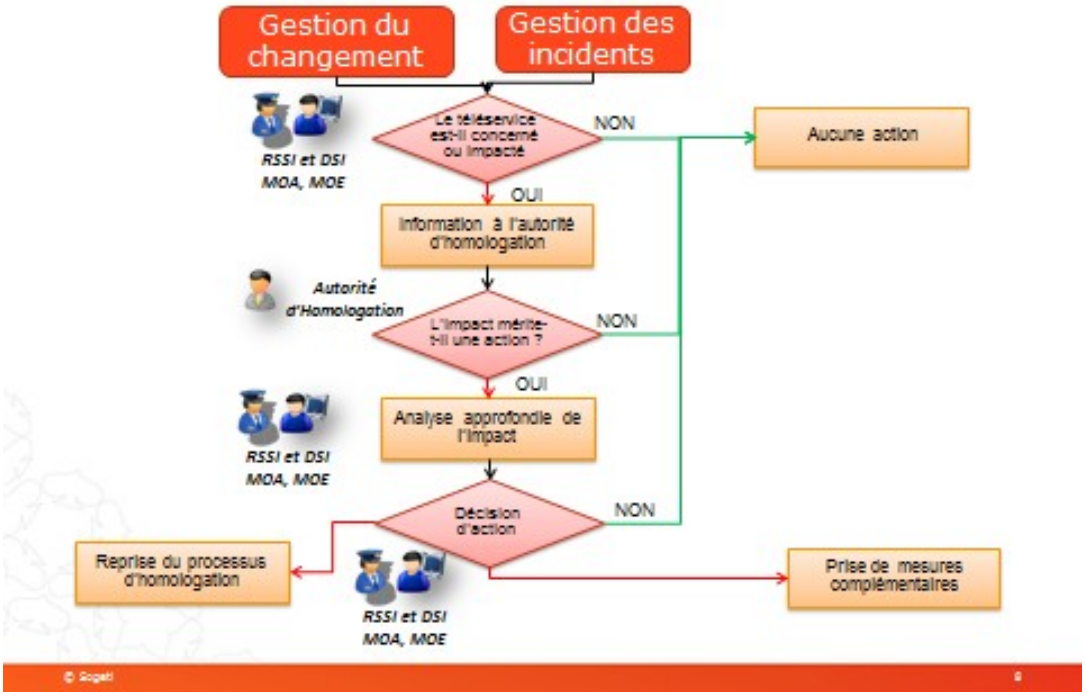
© Sogeti 

## La démarches d'homologation






## La démarche de révision



## Constitution du dossier remis à la commission

| Document du dossier d'homologation | Etat |
|---|---|
| Stratégie d'homologation | Document joint |
| Référentiel de sécurité | RGS + PSSI-E + PSSI |
| Risques identifiés (Le rapport d'analyse de risques) | Document joint |
| Politique de sécurité des systèmes d'information | PSSI de la Mairie |
| Procédures d'exploitation sécurisées du système | Référence jointe |
| Certificats de qualification des produits et prestataires | Dérogation |
| Risques résiduels (Le rapport d'analyse de risques) | Document joint |
| Décision d'autorisation d'exploitation (par famille). | Document joint |

© Sogeti


## Rapport d'analyse de risques

| Risque mitigé | Vraisemblance | Gravité | Risque |
|---|---|---|---|
| perte de Traçabilité sur Accès aux applications de la mairie d'après profil, en VPN SSL (mot de passe) | 2 : Significative | 4 : Critique | 6 : Important |
| perte de Confidentialité sur Billetterie en ligne | 2 : Significative | 2 : Limité | 4 : Limité |
| perte de Disponibilité sur Inscription aux centres de loisir | 2 : Significative | 2 : Limité | 4 : Limité |
| perte d'Intégrité sur Inscription aux centres de loisir | 2 : Significative | 2 : Limité | 4 : Limité |
| perte de Confidentialité sur Inscription aux centres de loisir | 2 : Significative | 2 : Limité | 4 : Limité |
| perte d'Intégrité sur Plateforme d'échange avec les fournisseurs | 2 : Significative | 2 : Limité | 4 : Limité |
| perte de Confidentialité sur Formulaire électronique sans authentification | 2 : Significative | 2 : Limité | 4 : Limité |
| perte d'Intégrité sur Ecrire au maire | 2 : Significative | 2 : Limité | 4 : Limité |
| perte de Confidentialité sur Ecrire au maire | 2 : Significative | 2 : Limité | 4 : Limité |
| perte de Confidentialité sur Gestion des concessions funéraires | 2 : Significative | 2 : Limité | 4 : Limité |
| perte de Traçabilité sur Billetterie en ligne | 1 : Minime | 2 : Limité | 3 : Faible |
| perte de Traçabilité sur Inscription aux centres de loisir | 1 : Minime | 2 : Limité | 3 : Faible |

© Sogeti

## Couverture des exigences DGME / RGS

| FONCTION DE SECURITE | | Mise en place de la fonction | Mécanisme choisi | JUSTIFICATION | Référence exigence DGME |
|---|---|---|---|---|---|
| Authentification | d'une personne | Oui | Par identifiants et mot de passe statiques | | [APP_AU], [DATA_OA] , [DATA_PA], [DATA_IN] |
| | Serveur | Oui | Avec certificat électronique | | [DATA_OA] , [DATA_PA], [DATA_IN] |
| Signature electronique | d'une personne | Non | Sans certificat électronique | Non concerné | |
| | Cachet serveur | Non | Sans certificat électronique | Non concerné | |
| Confidentialité | Chiffrement du canal | Oui | Avec certificat électronique | HTTPS | [DATA_CO], [APP_CO], [APP_CL] |
| Horodatage | Contremarque de temps | Non | Sans certificat électronique | Non concerné | |

| | | | |
|---|---|---|---|
| Niveau RGS Elevé | ** ou *** | | Risque fort et très fort |
| Niveau RGS Standard | * ou ** | | Risque moyen et fort |
| Niveau RGS Minimal | - | | Risque faible |



## Aspects dérogatoires

- Le certificat actuel qui utilise la signature SHA-1 a perdu son agrément en Août 2013. Comme il expire a l'automne 2017, il est accepté que ce certificat continue d'être utilisé jusqu'à son renouvellement.

## Proposition de délibération

- Tenant compte de la criticité des données traitées et des moyens déjà mis en place la commission propose l'homologation des télé-services sous réserves de mise en œuvre des mesures suivantes sous 12 mois:

| Code | Mesure à prendre | Commentaire |
|---|---|---|
| A-001 | Authentification forte pour les utilisateurs internes en VPN | Cette mesure a pour but d'éviter l'accès illimité par un pirate ou un partenaire. |
| A-002 | Ouverture dynamique du canal pour les partenaires | Cette mesure à pour but de conserver une authentification faible pour les partenaires. Chaque accès sera activé à la demande. |
| A-003 | Contractualiser les relations avec les partenaires incluant un accord de confidentialité | Cette mesure a pour but de sensibiliser les partenaires à la sécurité |
| A-004 | Formaliser les procédures d'exploitation des systèmes | Cette mesure a pour but de garantir un traitement efficace des reprises sur incident |
| A-005 | Imposer des mots de passe complexes (ou clavier virtuel) pour les accès partenaires | Cette mesure à pour but de limiter le risque d'usurpation d'identité |
| A-006 | Remplacer les comptes génériques des partenaires par des comptes individuels | Cette mesure a pour but d'assurer la traçabilité des accès et limiter l'usurpation de droits |

© Sogeti

# Publication de l'homologation

- La décision d'homologation devant être rendue accessible aux utilisateurs du télé-service, elle fait l'objet d'une publicité sur le support correspondant au télé-service (application, internet...).
- Voici un exemple de Mention Légales pour chaque télé-service homologué :
  - Homologation au titre du RGS:
    - Ce télé-service est conforme au Référentiel Général de Sécurité et a fait l'objet d'une décision d'homologation à la date du 01 juillet 2016, et ce, pour une durée de 3 ans.
    - Ci-joint la délibération de la collectivité *(lien vers la délib)*.

© Sogeti

## HOMOLOGATION RGS

La commission d'homologation, réunie en date du 01/07/2016, sur la base du dossier de sécurité présenté en séance, atteste la conformité RGS du téléservice xxx  pour une durée de  3 ans.
L'attestation d'homologation est téléchargeable ici.




# Analyse de risque

# des télé-services

# de la ville de Clermont-Ferrand

**Version : 1.0**

**Annexe N°2 de la délibération n° du 14/04/2017**

| | |
|---|---|
| Rédaction | Raphael AMADELLI<br>Signature |
| Vérification | Philippe BOST RSSI<br>Signature |
| Approbation | Jérôme AUSLENDER Elus Adjoints<br>Signature |

# Résumé de l'analyse

## Etude du contexte

### Cadre de la gestion du risque

Ce document constitue l'analyse de risque des télé-services de la ville de Clermont-Ferrand, rendu nécessaire pour l'homologation RGS de ces télé-services.

### Préparer les métriques

L'étude s'est attachée à déterminer les métriques de la sécurité avec les niveaux pour chacun des critères (Disponibilité, Intégrité, Confidentialité, traçabilité) définis par les directions métiers de la ville de Clermont-Ferrand.

### Identifier les biens et les mesures existantes

**10** Biens essentiels ont été identifiés
**22** Biens support ont été recensés, et leurs liens avec les biens essentiels établis
**3** Mesures existantes ont été identifiées

### Etude des évènements redoutés

**12** Evènements redoutés ont été retenus parmi 36 (ceux dont la gravité n'est pas négligeable), et classés par gravité :

| Gravité | |
|---|---|
| 4 : Critique | 1 |
| 3 : Important | |
| 2 : Limité | 11 |
| 1 : Négligeable | 25 |

## Etude des scénarios de menaces

**33** Scénarios de menace ont été retenus parmi les 37 calculés, retenus sur des critères d'applicabilité au contexte, jugés et classés par vraisemblance et vulnérabilité :

| Vraisemblance | |
|---|---|
| 4 : Maximale | |
| 3 : Forte | 6 |
| 2 : Significative | 7 |
| 1 : Minime | 24 |

## Analyser les risques

Une première approche a identifié le risque pour chaque évènement redouté comme suit :

| Risques actuels | |
|---|---|
| 8 : Critique | |
| 7 : très important | |
| 6 : Important | 1 |
| 5 : Sensible | |
| 4 : Limité | 9 |
| 3 : Faible | 2 |
| 2 : Très faible | |
| 1 : Négligeable | |

## Etude des mesures de sécurité

**2** Mesures de sécurité supplémentaires restant à mettre en œuvre ont été déduite de cette analyse :

Ces actions pour améliorer les mesures de sécurité ont été déterminées, et peuvent être classées comme suit :

| Efficacité actions | |
|---|---|
| 4 : Très efficace | 2 |
| 3 : Efficace | |
| 2 : Sensible | |
| 1 : Insignifiant | |

Pour chaque mesure un niveau d'efficacité sur chaque évènement redouté a été affecté, puis l'analyse par évènement redouté à permis d'évaluer puis de classifier les risques résiduels (risques restant après application des mesures), liés à chaque évènement redouté.

Seuls les évènements redoutés dont la gravité est vitale ou le risque important ont été analysés dans cette 2ième phase.

A l'issue de cette analyse, la répartition des nivaux de risque résiduels par évènement redouté est :

| Risques résiduels | |
|---|---|
| 8 : Critique | |
| 7 : très important | |
| 6 : Important | |
| 5 : Sensible | 1 |
| 4 : Limité | 9 |
| 3 : Faible | 2 |
| 2 : Très faible | |
| 1 : Négligeable | |

Le niveau de risques résiduels a été jugé acceptable et compatible avec les objectifs de sécurité lors de la réunion de présentation des résultats de la présente analyse.

# SOMMAIRE


**EXTRAIT DU REGISTRE DES DÉLIBÉRATIONS....1**

**OBJET : HOMOLOGATION DE TÉLÉ-SERVICES MIS EN OEUVRE AU SEIN DE LA VILLE DE CLERMONT-FERRAND....1**

**EN APPLICATION DE L'ORDONNANCE DITE « TÉLÉ-SERVICES » DU 8 DÉCEMBRE 2005 RELATIVE AUX ÉCHANGES ÉLECTRONIQUES ENTRE LES USAGERS ET LES AUTORITÉS ADMINISTRATIVES ET ENTRE LES AUTORITÉS ADMINISTRATIVES, IL VOUS EST PROPOSÉ L'HOMOLOGATION DE TROIS TÉLÉ-SERVICES MIS EN OEUVRE AU SEIN DE LA COLLECTIVITÉ. ....1**

*HOMOLOGATION RGS....12*

**ANNEXE N°2 DE LA DÉLIBÉRATION N° DU 17/02/2017....13**

**1.ETUDE DU CONTEXTE....19**

1.1.CADRE DE LA GESTION DU RISQUE....19
*1.1.1.Cadrage de l'étude de risques ....19*
*1.1.2.Périmètre de l'étude....20*
*1.1.3.Paramètres à prendre en compte....20*
1.2.PRÉPARER LES MÉTRIQUES....21
*1.2.1.Définir les critères de sécurité et élaborer les échelles de besoin....21*
*1.2.2.Elaborer une échelle de niveau de gravité....22*
*1.2.3.Elaborer une échelle de niveau de vraisemblance....22*
*1.2.4.Définir les critères de gestion du risque....23*
1.3.IDENTIFIER LES BIENS....24
*1.3.1.Identifier les biens essentiels, leurs relations et leurs dépositaires....24*
*1.3.2.Identifier les biens support, leurs relations et leurs propriétaires....27*
*1.3.3.Déterminer les liens entre biens essentiels et biens support....27*
*1.3.4.Déterminer les mesures de sécurité existantes....27*

**2.ETUDE DES ÉVÈNEMENTS REDOUTÉS....28**

2.1.ANALYSER ET ÉVALUER (EN TERME DE GRAVITÉ) TOUS LES ÉVÈNEMENTS REDOUTÉS....28

**3.ETUDE DES SCÉNARIOS DE MENACES....29**

3.1.ANALYSER ET ÉVALUER TOUS LES SCÉNARIOS DE MENACES....29

**4.APPRÉCIER LES RISQUES....30**

4.1.ANALYSER ET ÉVALUER LES RISQUES, OPTIONS DE TRAITEMENT....30
4.2.IDENTIFIER LES OBJECTIFS DE SÉCURITÉ....31

**5.ETUDE DES MESURES DE SÉCURITÉ....32**

5.1.FORMALISER LES MESURES DE SÉCURITÉ À METTRE EN ŒUVRE....32
*5.1.1.Déterminer les mesures de sécurité....32*
5.2.METTRE EN ŒUVRE LES MESURES DE SÉCURITÉ....32
*5.2.1.Etablir un plan d'action et suivre la réalisation....32*
*5.2.2.Analyser les risques résiduels....33*

**6.ANNEXES....35**

6.1.BIENS SUPPORT ET LIENS AVEC LES BIENS ESSENTIELS....36
6.2.MESURES EXISTANTES....54
6.3.EVÈNEMENTS REDOUTÉS....55
6.4.VULNÉRABILITÉS....60
6.5.MENACES....62
6.6.MESURES RESTANT À PRENDRE....63

# Index des tableaux

# Index des figures

# PREAMBULE

La présente analyse de risque a été réalisée pour constituter le dossier d'homologation RGS des télé-services. Elle a été réalisée en utilisant la méthode EBIOS version 2010 de l'ANSSI.

La décision d'homologation devant être rendue accessible aux utilisateurs du télé-service, elle fait l'objet d'une publicité sur le support correspondant au télé-service (application, internet...).

Voici un exemple de Mention Légales pour chaque télé-service homologué :

Homologation au titre du RGS:

Ce télé-service est conforme au Référentiel Général de Sécurité et a fait l'objet d'une décision d'homologation à la date du 01 juillet 2016, et ce, pour une durée de 3 ans.

Ci-joint la délibération de la collectivité (lien vers la délib).

## La Méthode EBIOS de l'ANSSI

La démarche EBIOS est composée de 5 modules. Les chapitres du présent document reprennent la numérotation des modules telle qu'elle est définie dans la méthode. Les s'enchaînent selon le schéma suivant :

**Figure 1 – Schéma de la méthode EBIOS**

## Module 1 : Étude du contexte.

Ce module permet d'étudier le contexte du système cible. (Contexte général , Périmètre de l'étude, Hypothèses, Contraintes, Sources de menaces, Métriques (critère de sécurité, Echelle DIC – gravité et vraisemblance), Bien essentiel (processus, informations et dépositaires), Biens supports, Lien entre biens essentiels et biens supports, et des mesures existantes.

## Module 2 : Étude des événements redoutés.

Chaque bien essentiel identifié dans le module 1 fournit des évènements redouté dans les catégories:

- indisponibilité.
- altération (intégrité).
- compromission (confidentialité).

A chaque événement redouté est associé :

- le besoin de sécurité. (DICT)
- des sources de menaces.
- des impacts.

La gravité est estimée sur chaque événement redouté.

## Module 3 : Etude des scénarios de menaces.

Chaque bien support identifié dans le module 1 donne des scénarios de menace dans les catégories:

- indisponibilité.
- altération (intégrité).
- compromission (confidentialité).

Pour chaque scénario de menace sont associées les sources de menaces.

La vraisemblance est estimée sur chaque événement redouté.

Des méthodes d'attaques sont mises à titre d'exemple (Base de connaissance – Menaces et Vulnérabilité Générique).

## Module 4 : Etude des risques.

Chaque événement redouté donne lieu à un risque. A chaque risque est associé un Niveau de risque. Celui-ci est déterminé à l'aide de :

- la gravité de l'événement redouté associé au risque.
- la vraisemblance des scénarios de menaces associées au risque

Chaque risque fait l'objet d'une réévaluation globale de la vraisemblance et de la gravité en fonction des scénarios de menaces et des mesures existantes, puis d'un choix de traitement (Evitement, Réduction, Prise, Transfert)

## Module 5 : Etude des mesures de sécurité.

Les mesures de sécurité sont établies afin de réduire les risques. Elles sont étudiées sur la base du référentiel ISO 27002 et permettent une des lignes de défense suivantes :

- Prévenir (se prémunir contre l'apparition des incidents et sinistres).
- Protéger (détecter, bloquer et contenir).

Récupérer (minimiser les conséquences des incidents et des sinistres).

Les mesures de sécurité permettent également, par rapprochement avec les évènements redoutés, d'évaluer le risque résiduel une fois qu'elles seront en place.

# 1.ETUDE DU CONTEXTE

## 1.1.Cadre de la gestion du risque

### 1.1.1.Cadrage de l'étude de risques

#### 1.1.1.1.Description du système

Le système objet de la présente analyse de risque représente l'ensemble des composants entrant dans les télé-services opérés par la ville de Clermont-Ferrand.

Le système d'information analysé est composé de la manière suivante :

- Un site hébergé par l'opérateur local NEYRIAL qui offre un service de type PaaS sur lequel la ville a installé les composants logiciels d'un portail et les programmes spécifiques pour accepter les requêtes en provenance d'Internet et à destination du site « ville-clermont-ferrand.fr ».
- Un site hébergé dans les locaux de la mairie qui accueille directement les requêtes des applications Smartphone et Tablette, et son backup en cas de PCA.
- Une interface entre le site NEYRIAL et le site de la mairie qui transmet immédiatement et sans les mémoriser l'ensemble des données reçues sur le portail.
- Des liens avec des sites partenaires avec des échanges de données mono ou bidirectionnelles :
  - Rodrigue pour la billetterie des spectacles. Les bases de données des abonnés sont stockées sur le site de la mairie et consultées par Rodrigue lors de l'achat de billets. Les places confiées à Rodrigue sont saisies sur le site de Rodrigue par la mairie. Rodrigue renvoie le paiement des places vendues.
  - Muse pour la gestion du conservatoire, pour lequel la mairie n'est que client, et se contente de fournir les liens vers ce prestataire. Ce fonctionnement l'exclut du périmètre de la présente analyse de risque. Pour autant, le prestataire doit apporter les éléments de preuve de sa conformité RGS.
  - TIPI pour le paiement en ligne. La mairie ne fait que rediriger vers ce centre de paiement de l'état, qui est homologué.
  - GEDICOM, qui est un organisme permettant de gérer les envois de SMS et appels en cas de gestion de crise, pour lequel la ville enregistre les demandes et les retransmet à GEDICOM.
  - PVE (Envoi des PV au centre national pour lequel la ville n'est que client, ce qui l'exclut du champ de la présente analyse)

#### 1.1.1.1.Missions du système

Les missions du système sont d'apporter du confort aux usagers dans leurs démarches administratives ou inscriptions, ainsi que de permettre un dialogue direct avec les services sans se déplacer.

#### 1.1.1.2.Fonctions du système

Les fonctions offertes par le système sont directement liées aux processus métier. Le détail précis de ces fonctions est décrit dans les comptes-rendus d'entretien, et résumés ci-après :

- Télé-services sans authentification permettant d'accomplir des démarches de type demandes ou information à destination des services de la mairie.
- Télé-services avec authentification permettant d'accéder à des fonctions spécifiques à usage familial ou professionnel, dont la confidentialité et l'intégrité des données peut dépendre de la fonction accédée, et doit donc être contrôlée avec attention.

#### 1.1.1.1.Liaison et interopérabilité avec les autres systèmes

NEYRIAL : C'est le prestataire qui héberge le portail. Il envoie les données recueillies sur le site de la mairie au format HTTPS.

RODRIGUE : c'est le prestataire de billetterie avec lequel les échanges se font comme suit :

- La Mairie envoie les éléments sur le spectacle qu'elle organise et confie un certain nombre de place à vendre à Rodrigue
- Rodrigue consulte la base de données des abonnés pour la gestion des tarifs de vente.
- Rodrigue envoie les paiements des sommes perçues à la Mairie

#### 1.1.1.1.Agréments et cautions

La validation de ce document est réalisée par Philippe BOST DSI/RSSI

L'approbation est réalisée par Jérôme AUSLENDER Elus Adjoints.

### 1.1.2.Périmètre de l'étude

La présente analyse de risque concerne l'ensemble des composants du système d'information de la Mairie de Clermont-Ferrand qui sont concernés par la mise en œuvre des télé-services.

### 1.1.3.Paramètres à prendre en compte

#### 1.1.3.1.Contraintes d'ordre techniques et règlementaires

La Mairie de Clermont-Ferrand doit respecter l'ensemble des directives et textes suivants :

| | Titre | Référence |
|---|---|---|
| **[PSSI-E]** | Politique de sécurité de l'état | Version du 20 Février 2014 |
| **[RGS]** | Référentiel Général de Sécurité V 2 | Version du 13/06/2014 |
| **[PSSI]** | PSSI de la Mairie de Clermont-Ferrand | Version 2010 |

**Tableau 1 – Textes applicables**

#### 1.1.3.2.Contraintes de personnel

Les personnels de la mairie concernés par les biens essentiels et biens support du périmètre analyse sont :

| Code | Fonction | Nom et Prénom |
|---|---|---|
| RSSI | Responsable sécurité | Mr BOST |
| DSI | Directeur informatique | Mr BOST |
| ADM1 | Administrateurs des télé-services | Administrateurs |
| RFUNR | Responsable fonctionnel "funeraire" | Mme GARDET |
| RINFRA | Responsable infrastructure | Mr AMADELLI |
| RBILL | Responsable billetterie | Mme BŒUF |
| ASPIP | Administrateur SPIP | Mr DIJOUX |
| ASQL | Responsables développements | Mr ANDREJEWSKI |
| AORA | Responsable ORACLE | Mr HOUE |
| RECVL | Responsable état civil | Mme NORMAND |
| RDRH | Direction des ressources humaines | Mr THEURET |
| RDEP | Direction technique | Mr MALAYRAT |
| RCABM | Responsable du cabinet du maire | Mme CHAUMEIL |
| EFAMIL | Responsable espace famille | Mme ESSABIR |

**Tableau 2 – Personnes concernées par l'analyse de risque**

#### 1.1.3.3.Contraintes calendaires

L'homologation RGS V2 doit être prononcée avant le 1er juillet 2016.

## 1.2.Préparer les métriques

L'ensemble des métriques sont décrites dans les annexes techniques « **Métrique** ». Pour les critères les plus importants, la métrique est rappelée ci-après.

### 1.2.1.Définir les critères de sécurité et élaborer les échelles de besoin

Les critères retenus sont les mêmes que ceux retenus par la PSSI du ministère de la santé, avec toutefois des échelles ajustées aux besoins spécifique de la Mairie de Clermont-Ferrand.

- Disponibilité
- Intégrité
- Confidentialité
- Traçabilité

Pour chacun de ces critères, les niveaux sont définis et explicités comme suit :

| D | Métrique Disponibilité |
|---|---|
| 1 : Minime | Indisponibilité acceptable de 1 semaine |
| 2 : Nécessaire | Indisponibilité acceptable de 3 jours |
| 3 : Critique | Indisponibilité acceptable de 1 journée |
| 4 : Vitale | Indisponibilité acceptable de 4 heures |

| I | Métrique Intégrité |
|---|---|
| 1 : Minime | Peut ne pas être intègre |
| 2 : Détectable | Peut contenir des erreurs si elles sont identifiées |
| 3 : Maîtrisée | Peut contenir des erreurs si on peut les retrouver et les corriger |
| 4 : Prouvée | Doit être rigoureusement intègre et son intégrité doit-être prouvée. |

| C | Métrique Confidentialité |
|---|---|
| 1 : Public | Donnée publique ne nécessitant pas de protection particulière |
| 2 : Restreint | Ne doit être accessible qu'au personnel et aux partenaires. |
| 3 : Confidentiel | Ne doit être accessible qu'aux personnes impliquées. |
| 4 : Secret | Accessible qu'à des personnes identifiées et ayant le besoin d'en connaître. |

| T | Métrique Traçabilité |
|---|---|
| 1 : Minimum | Besoin de traçabilité pour information |
| 2 : Nécessaire | L'action doit être tracée: l'entité doit être identifiée. |
| 3 : Essentielle | L'action doit être tracée: L'auteur doit être identifié |
| 4 : Opposable | L'action doit être tracée pour servir de preuve opposable. |

**Tableau 3 – Métriques disponibilité, intégrité, confidentialité et traçabilité**

### 1.1.1. Elaborer une échelle de niveau de gravité

La gravité d'un évènement redouté est définie comme suit :

| Métrique gravité d'impact | |
|---|---|
| 1 : Négligeable | L'impact sera facilement surmonté |
| 2 : Limité | Nécessite la mise en place de mesures de contournement mineures |
| 3 : Important | Nécessite la mise en place de mesures de contournement majeures |
| 4 : Critique | Remise en cause de la mission |

**Tableau 4 – Métrique gravité d'impact**

### 1.1.2. Elaborer une échelle de niveau de vraisemblance

La vraisemblance d'un scénario de sinistre est définie en fonction de la facilité d'exploitation d'une vulnérabilité et de l'occurrence d'apparition d'une menace, comme suit :

| Métrique facilité d'exploitation d'une vulnérabilité | |
|---|---|
| 1 : Très complexe | Il faut un niveau d'expertise et/ou de connaissance du contexte très fort |
| 2 : Complexe | Il faut une expertise et/ou une connaissance du contexte |
| 3 : Moyenne | Il faut un certain travail de recherche |
| 4 : Aisée | Possible sans expertise ni connaissance du contexte |

**Tableau 5 – Métrique facilité d'exploitation d'une vulnérabilité**

| Métrique occurrence d'apparition d'une menace | |
|---|---|
| 1 : Exceptionnel | Ne devrait pas en principe arriver (ex: crue centennale) |
| 2 : Probable | Arrivera à moyen terme (notion d'années) |
| 3 : Courant | Arrive régulièrement (notion de semaines, mois) |
| 4 : Permanente | Arrive tout le temps (notion jours, voire heures) |

**Tableau 6 – Métrique Occurrence d'apparition d'une menace**

| Vraisemblance | |
|---|---|
| 1 : Minime | Un hacker peut tomber dessus par hasard,<br>La cause accidentelle n'a quasiment aucune chance de se produire |
| 2 : Significative | Des personnes malveillantes peuvent avoir un intérêt à agir sur le système,<br>Il existe une faible probabilité que la cause accidentelle survienne |
| 3 : Forte | Il existe des personnes menaçant le système,<br>La cause accidentelle peut facilement survenir |
| 4 : Maximale | Le système intéresse fortement des personnes malveillantes,<br>La cause accidentelle risque fortement de survenir |

**Tableau 7 – Métrique de vraisemblance**

| Vraisemblance (combine facilité d'exploitation et occurrence) | | | |
|---|---|---|---|
| Facilité<br>Occurrence | 1 : Très complexe | 2 : Complexe | 3 : Moyenne |
| 1 : Exceptionnel | 1 : Minime | 1 : Minime | 2 : Significative |
| 2 : Probable | 1 : Minime | 2 : Significative | 3 : Forte |
| 3 : Courant | 2 : Significative | 3 : Forte | 3 : Forte |
| 4 : Permanente | 2 : Significative | 3 : Forte | 4 : Maximale |

**Tableau 8 – Vraisemblance fonction de la facilité (vulnérabilité) et de l'occurrence (menace)**

### 1.1.3. Définir les critères de gestion du risque

Les critères de gestion du risque permettent notamment d'estimer et d'évaluer les risques et de prendre les décisions concernant leur appréciation et leur traitement.

| Critère | Description |
|---|---|
| Estimation des événements redoutés (module 2) | •Les événements redoutés sont estimés en termes de gravité à l'aide de l'échelle définie à cet effet |
| Évaluation des Scénarios de menaces (module 3) | •Les scénarios de menaces sont classés par ordre décroissant de vraisemblance. |
| Estimation des risques (module 4) | •La gravité d'un risque est égale à celle de l'événement redouté.<br>•La vraisemblance d'un risque est égale à la maximale de tous les scénarios de menaces liés à l'événement redouté. |
| Évaluation des risques (module 4) | •Le niveau de risque est établi selon l'échelle définie à cet effet<br>•Il est calculé selon la matrice gravité/vraisemblance<br>•Le traitement préconisé est établi selon la gravité/vraisemblance |

Le niveau de risque est défini comme suit :

| Métrique risque | |
|---|---|
| 1 : Négligeable | Le risque peut ne pas être pris en compte |
| 2 : Très faible | Le risque est à traiter en priorité basse |
| 3 : Faible | Le risque est à traiter en priorité basse |
| 4 : Limité | Le risque est à traiter en priorité moyenne |
| 5 : Sensible | Le risque est à traiter en priorité moyenne |
| 6 : Important | Le risque est à traiter en priorité haute |
| 7 : très important | Le risque est à traiter en priorité absolue |
| 8 : Critique | Le niveau de risque est inacceptable |

**Tableau 9 – Métrique de niveau de risque**

Ce niveau de risque est calculé d'après une matrice gravité/vraisemblance définie comme suit :

| Niveau de risque : Combine Impact et vraisemblance | | | |
|---|---|---|---|
| Impact<br>Vraisemblance | 1 : Négligeable | 2 : Limité | 3 : Important |
| 1 : Minime | 1 : Négligeable | 3 : Faible | 4 : Limité |
| 2 : Significative | 3 : Faible | 4 : Limité | 5 : Sensible |
| 3 : Forte | 4 : Limité | 5 : Sensible | 6 : Important |
| 4 : Maximale | 5 : Sensible | 6 : Important | 7 : très important |

**Tableau 10 – Niveau de risque fonction de la vraisemblance et de la gravité**

Pour chaque niveau de risque le traitement « préconisé » est défini comme suit :

| Traitement du risque : Combine Impact et vraisemblance | | | |
|---|---|---|---|
| Impact<br>Vraisemblance | 1 : Négligeable | 2 : Limité | 3 : Important |
| 1 : Minime | Prendre | Prendre | Réduire |
| 2 : Significative | Prendre | Prendre | Réduire |
| 3 : Forte | Prendre | Réduire | Réduire |
| 4 : Maximale | Réduire | Réduire | Eviter |

**Tableau 11 – Traitement préconisé fonction de la vraisemblance et de la gravité**

## 1.1.Identifier les biens

### 1.1.1.Identifier les biens essentiels, leurs relations et leurs dépositaires

Chaque bien essentiel est décrit par :

- Un code d'identification
- La description du bien
- Le besoin en sécurité (D.I.C.T.)
- Les informations essentielles concernées

**10** Biens essentiels ont été retenus dans la liste de ceux initialement identifiés

| Code | Type | Retenu | **Bien essentiel** | Besoin sécurité | Commentaires, fonction ou Informations essentielles concernées |
|---|---|---|---|---|---|
| B-BILLET | Fonction | Oui | Billetterie en ligne | D=3 : Critique<br>I=3 : Maîtrisée<br>C=3 : Confidentiel<br>T=3 : Essentielle | Service acheté à la billeterie RODRIGUE, mais base de donnée stockée à lamairie |
| C-EFTAG | Fonction | Oui | Demander l'effacement de tags | D=2 : Nécessaire<br>I=2 : Détectable<br>C=2 : Restreint<br>T=1 : Minimum | |
| C-FUNER | Fonction | Oui | Gestion des concessions funéraires | D=3 : Critique<br>I=3 : Maîtrisée<br>C=3 : Confidentiel<br>T=1 : Minimum | S'adresse aux professionnels, avec login |
| E-CLOUD | Fonction | Oui | Plateforme d'échange avec les fournisseurs | D=2 : Nécessaire<br>I=3 : Maîtrisée<br>T=3 : Essentielle | |
| E-PROC | Processus | Oui | Formulaire électronique sans authentification | D=3 : Critique<br>I=2 : Détectable<br>C=3 : Confidentiel<br>T=2 : Nécessaire | D-NAISS : Demander un acte de naissance<br>D-MARIA : Demander un acte de mariage<br>D-DECES : Demander un acte de décès<br>D-PASSP : Demander un rendez-vous passeport / CNI |
| EXTRANET | Fonction | Oui | Accès aux applications de la mairie d'après profil, en VPN SSL (mot de passe) | D=3 : Critique<br>T=4 : Opposable | |
| I-LOISIR | Fonction | Oui | Inscription aux centres de loisir | D=3 : Critique<br>I=3 : Maîtrisée<br>C=3 : Confidentiel<br>T=3 : Essentielle | Espace famille (Kiosque) |
| M-MAIRE | Fonction | Oui | Ecrire au maire | D=3 : Critique<br>I=2 : Détectable<br>C=3 : Confidentiel<br>T=3 : Essentielle | N'existe que sur l'appli mobile |

| Code | Type | Retenu | **Bien essentiel** | Besoin sécurité | Commentaires, fonction ou Informations essentielles concernées |
|---|---|---|---|---|---|
| O-EMPLOI | Processus | Oui | Consulter et postuler aux offres d'emploi | D=2 : Nécessaire<br>I=2 : Détectable<br>C=3 : Confidentiel<br>T=2 : Nécessaire | O-ANIMA : Candidater comme animateur occasionnel |
| S-ANOMA | Fonction | Oui | Signaler une anomalie sur espace public | D=2 : Nécessaire<br>I=2 : Détectable<br>C=2 : Restreint<br>T=1 : Minimum | |
| A-CRISE | Fonction | Non | S'inscrire à l'alerte gestion de crise | D=2 : Nécessaire<br>I=3 : Maîtrisée<br>C=2 : Restreint<br>T=2 : Nécessaire | GEDICOM |
| C-PARK | Fonction | Non | Disponibilité des parkings | | N'est pas considéré comme un télé-service mais comme un simple site d'information |
| C-PLPOS | Fonction | Non | Consulter le plan de ville et le POS | | N'est pas considéré comme un télé-service mais comme un simple site d'information |
| C-WCAM | Fonction | Non | WEBCams de la ville | | N'est pas considéré comme un télé-service mais comme un simple site d'information |
| D-ACTES | Fonction | Non | Dématérialisation des actes | | Plateforme d'échange externe avec la prefecture |
| D-DECES | Fonction | Non | Demander un acte de décès | D=3 : Critique<br>I=2 : Détectable<br>C=3 : Confidentiel<br>T=2 : Nécessaire | |
| D-MARIA | Fonction | Non | Demander un acte de mariage | D=3 : Critique<br>I=2 : Détectable<br>C=3 : Confidentiel<br>T=2 : Nécessaire | |
| D-NAISS | Fonction | Non | Demander un acte de naissance | D=3 : Critique<br>I=2 : Détectable<br>C=3 : Confidentiel<br>T=2 : Nécessaire | |

| Code | Type | Retenu | **Bien essentiel** | Besoin sécurité | Commentaires, fonction ou Informations essentielles concernées |
|---|---|---|---|---|---|
| D-PASSP | Fonction | Non | Demander un rendez-vous passeport / CNI | D=3 : Critique<br>I=2 : Détectable<br>C=2 : Restreint<br>T=2 : Nécessaire | |
| G-PVE | Fonction | Non | Gestion des PV électroniques | | Gestion nationale |
| I-MUSE | Fonction | Non | Gestion du conservatoire | | Service acheté |
| M-MARPU | Fonction | Non | Consulter et répondre aux marchés publics | | Se contente de rediriger vers le site qui gère les marchés publics |
| O-ANIMA | Fonction | Non | Candidater comme animateur occasionnel | D=2 : Nécessaire<br>I=2 : Détectable<br>C=3 : Confidentiel<br>T=2 : Nécessaire | |
| P-STIPI | Fonction | Non | Paiement en ligne des services municipaux | | Se contente de renvoyer sur TIPI |
| S-PROJET | Fonction | Non | Suivi de projets et parrainage jeunes | | Obsolète |
| T-FORMU | Fonction | Non | Télécharger un formulaire | | N'est pas considéré comme un télé-service mais comme un simple site de téléchargement |

**Tableau 12 – Liste des biens essentiels**

### 1.1.1. Identifier les biens support, leurs relations et leurs propriétaires

Chaque bien support à prendre en comptes est décrit par :

- Un code
- Le type de bien issu de la table précédente
- Une description

**22** Biens support ont été recensés, et leurs liens avec les biens essentiels établis. La liste complète se trouve dans les annexes techniques « **Biens support** »

### 1.1.1. Déterminer les liens entre biens essentiels et biens support

Les relations entre biens essentiels et biens support sont également décrites dans l'annexe « **Biens support** ».

### 1.1.2. Déterminer les mesures de sécurité existantes

Chaque mesure existante est caractérisée par :

- Une description
- Les types de bien support sur lesquels la mesure agit
- Les critères de sécurité ((DICT) sur lesquels la mesure agit
- 3 indicateurs précisant s'il s'agit de mesures de prévention, protection ou récupération

L'efficacité de ces mesures a été estimée comme suit :

| Efficacité mesures | |
|---|---|
| 4 : Très efficace | 1 |
| 3 : Efficace | 1 |
| 2 : Sensible | 1 |
| 1 : Insignifiant | |

**Tableau 13 – Efficacité estimée des mesures existantes**

# 1.ETUDE DES ÉVÈNEMENTS REDOUTÉS

L'étude des évènements redoutés utilise le référentiel d'impacts précisé dans les annexes techniques « **Impacts** », avec pour chacun :

- Une famille (financier, juridique, image, …)
- Une description
- Une gravité

## 1.1.Analyser et évaluer (en terme de gravité) tous les évènements redoutés

Les évènements redoutés ont été étudiée pour chaque bien essentiel et chaque critère DICT affecté. L'annexe technique « **Evènements redouté** » présente pour chacun des évènements redoutés :

- La description de ce qui est redouté pour le bien essentiel
- Le bien essentiel affecté
- Le besoin en sécurité exprimé reprenant les critères DICT de la métrique
- Les impacts possibles parmi la liste « impacts » établie sur la base du référentiel
- La gravité calculée comme la gravité maximum de l'impact que cet événement redouté peut engendrer

**12** Evènements redoutés ont été retenus parmi 36 (ceux dont la gravité n'est pas négligeable), et classés par gravité :

| Gravité | |
|---|---|
| 4 : Critique | 1 |
| 3 : Important | |
| 2 : Limité | 11 |
| 1 : Négligeable | 25 |

**Tableau 14 – Classement des évènements redoutés par gravité**

# 1.ETUDE DES SCÉNARIOS DE MENACES

L'étude des scénarios de menaces s'appuie sur les référentiels de menaces et de vulnérabilités décrits dans les annexes techniques « **Menaces** » et « **Vulnérabilités** ».

Pour les vulnérabilités, ce tableau contient les informations :

- Un code
- Une description de la vulnérabilité
- Une information Oui ou Non si la vulnérabilité est retenue dans le cadre de cette étude

Pour les menaces, ce tableau contient les informations :

- Un code
- Une description de la menace
- Les critères DICT affectés
- Une information Oui ou Non si la menace est retenue dans le cadre de cette étude

## 1.1.Analyser et évaluer tous les scénarios de menaces

La liste complète des scénarios se trouve dans les annexes techniques « Scénarios de menaces ».

L'ensemble des combinaisons plausibles bien support/menace/vulnérabilité constitue la liste des scénarios de menace, avec pour chacun :

- La menace
- Le bien support concerné
- Les vulnérabilités potentiellement exploitées
- Les critères DICT affectés
- L'occurrence d'apparition
- La facilité d'exploitation de la vulnérabilité
- La vraisemblance déduite de la facilité et de l'occurrence

**33** Scénarios de menace ont été retenus parmi les 37 calculés, retenus sur des critères d'applicabilité au contexte, jugés et classés par vraisemblance et vulnérabilité :

| Vraisemblance | |
|---|---|
| 4 : Maximale | |
| 3 : Forte | 6 |
| 2 : Significative | 7 |
| 1 : Minime | 24 |

**Tableau 15 – Classement des scénarios par vraisemblance**

# 1.APPRÉCIER LES RISQUES

## 1.1.Analyser et évaluer les risques, options de traitement

L'appréciation des risques a été effectuée pour chaque évènement redouté, en prenant en compte l'ensemble des scénarios de menace qui s'y appliquent, pondérée par l'ensemble des mesures existantes.

La synthèse de l'analyse et de l'évaluation fait apparaître les risques suivants, classés par niveau décroissant, pour les risques à traiter en priorité d'après les objectifs de sécurité :

Les traitements préconisés sont déduits de la métrique risque en fonction de la gravité et vraisemblance, et conformes aux 4 traitements possibles de la norme ISO 27005

| Risques actuels | |
|---|---|
| 8 : Critique | |
| 7 : très important | |
| 6 : Important | 1 |
| 5 : Sensible | |
| 4 : Limité | 9 |
| 3 : Faible | 2 |
| 2 : Très faible | |
| 1 : Négligeable | |

**Tableau 16 – Nombre de risques actuels par niveau de risque**

| Risque mitigé | Vraisemblance | Gravité | Risque | Traitement |
|---|---|---|---|---|
| EXTRANET-T : perte de Traçabilité sur Accès aux applications de la mairie d'après profil, en VPN SSL (mot de passe) | 2 : Significative | 4 : Critique | 6 : Important | Transférer |
| B-BILLET-C : perte de Confidentialité sur Billetterie en ligne | 2 : Significative | 2 : Limité | 4 : Limité | Prendre |
| I-LOISIR-D : perte de Disponibilité sur Inscription aux centres de loisir | 2 : Significative | 2 : Limité | 4 : Limité | Prendre |
| I-LOISIR-I : perte d'Intégrité sur Inscription aux centres de loisir | 2 : Significative | 2 : Limité | 4 : Limité | Prendre |
| I-LOISIR-C : perte de Confidentialité sur Inscription aux centres de loisir | 2 : Significative | 2 : Limité | 4 : Limité | Prendre |
| E-CLOUD-I : perte d'Intégrité sur Plateforme d'échange avec les fournisseurs | 2 : Significative | 2 : Limité | 4 : Limité | Prendre |
| E-PROC-C : perte de Confidentialité sur Formulaire électronique sans authentification | 2 : Significative | 2 : Limité | 4 : Limité | Prendre |
| M-MAIRE-I : perte d'Intégrité sur Ecrire au maire | 2 : Significative | 2 : Limité | 4 : Limité | Prendre |
| M-MAIRE-C : perte de Confidentialité sur Ecrire au maire | 2 : Significative | 2 : Limité | 4 : Limité | Prendre |
| C-FUNER-C : perte de Confidentialité sur Gestion des concessions funéraires | 2 : Significative | 2 : Limité | 4 : Limité | Prendre |
| B-BILLET-T : perte de Traçabilité sur Billetterie en ligne | 1 : Minime | 2 : Limité | 3 : Faible | Prendre |
| I-LOISIR-T : perte de Traçabilité sur Inscription aux centres de loisir | 1 : Minime | 2 : Limité | 3 : Faible | Prendre |

**Tableau 17 – Classement des risques actuels par niveau de risque**

| | | | | | |
|---|---|---|---|---|---|
| Vraisemblance | 4 : Maximale | | | | |
| | 3 : Forte | | | | |
| | 2 : Significative | | B-BILLET-C<br>I-LOISIR-D<br>I-LOISIR-I<br>I-LOISIR-C<br>E-CLOUD-I<br>E-PROC-C<br>M-MAIRE-I<br>M-MAIRE-C<br>C-FUNER-C | | EXTRANET-T |
| | 1 : Minime | | B-BILLET-T<br>I-LOISIR-T | | |
| | | 1 : Négligeable | 2 : Limité | 3 : Important | 4 : Critique |
| | | Gravité d'impact | | | |

**Tableau 18 – Cartographie des risques actuels**

## 1.2.Identifier les objectifs de sécurité

Les objectifs de sécurité ont été déterminés comme suit :

---

**Le risque de risque après traitement doit être inférieur ou égale à limité.**

# 2.ETUDE DES MESURES DE SÉCURITÉ

## 2.1.Formaliser les mesures de sécurité à mettre en œuvre

### 2.1.1.Déterminer les mesures de sécurité

Les mesures de sécurité à mettre en œuvre ne concernent que le risque jugé important qui porte sur les télé-services avec authentification.

•L'authentification forte pour les employés de la mairie qui donne des droits supérieurs permet d'éviter l'usurpation d'identité par des utilisateurs dont les droits sont normalement restreints.

•L'ouverture dynamique du canal pour l'accès maintenance ou autre par les services de la mairie permet de contrôler ce qui est fait et quand lors des maintenances.

•La contractualisation des accords avec les partenaires.

•La formalisation des procédures d'exploitation.

| Efficacité actions | |
|---|---|
| 4 : Très efficace | 4 |
| 3 : Efficace | |
| 2 : Sensible | 1 |
| 1 : Insignifiant | |

**Tableau 19 – Classement des mesures restant à prendre**

La liste complète des mesures à prendre est décrite dans les annexes techniques « **Mesures à prendre** » Dans ce tableau, elles sont définies par :

•Un numéro d'ordre

•Une description

•Le bien support sur lequel elle porte

•Le thème ISO sur lequel elle porte

•3 indicateurs précisant s'il s'agit de mesures de prévention, protection ou récupération

•Une zone de commentaire

## 1.1.Mettre en œuvre les mesures de sécurité

### 1.1.1.Etablir un plan d'action et suivre la réalisation

L'annexe « **Actions** », présente les mesures restant à prendre pour atteindre les objectifs de sécurité elle comporte les informations :

•Description de la mesure à prendre

•Type de biens supports à laquelle la mesure s'applique

•Efficacité estimée

•Critères DICT affectés

### 1.1.1.Analyser les risques résiduels

L'annexe « **Résiduels** », permet d'identifier pour chaque risque l'ensemble des mesures restant à prendre, avec pour chacune une efficacité qui a été ré-estimée, et d'en déduire le risque résiduel.

A l'issue de l'analyse, les risques résiduels restants peuvent être identifiés comme suit (classés par risque décroissants) :

| Risques résiduels | |
|---|---|
| 8 : Critique | |
| 7 : très important | |
| 6 : Important | |
| 5 : Sensible | 1 |
| 4 : Limité | 9 |
| 3 : Faible | 2 |
| 2 : Très faible | |
| 1 : Négligeable | |

**Tableau 20 – Nombre de risques résiduels par niveau de risque**

| Risque résiduel | Vraisemblance | Gravité | Risque |
|---|---|---|---|
| EXTRANET-T : perte de Traçabilité sur Accès aux applications de la mairie d'après profil, en VPN SSL (mot de passe) | 1 : Minime | 4 : Critique | 5 : Sensible |
| B-BILLET-C : perte de Confidentialité sur Billetterie en ligne | 2 : Significative | 2 : Limité | 4 : Limité |
| I-LOISIR-D : perte de Disponibilité sur Inscription aux centres de loisir | 2 : Significative | 2 : Limité | 4 : Limité |
| I-LOISIR-I : perte d'Intégrité sur Inscription aux centres de loisir | 2 : Significative | 2 : Limité | 4 : Limité |
| I-LOISIR-C : perte de Confidentialité sur Inscription aux centres de loisir | 2 : Significative | 2 : Limité | 4 : Limité |
| E-CLOUD-I : perte d'Intégrité sur Plateforme d'échange avec les fournisseurs | 2 : Significative | 2 : Limité | 4 : Limité |
| E-PROC-C : perte de Confidentialité sur Formulaire électronique sans authentification | 2 : Significative | 2 : Limité | 4 : Limité |
| M-MAIRE-I : perte d'Intégrité sur Ecrire au maire | 2 : Significative | 2 : Limité | 4 : Limité |
| M-MAIRE-C : perte de Confidentialité sur Ecrire au maire | 2 : Significative | 2 : Limité | 4 : Limité |
| C-FUNER-C : perte de Confidentialité sur Gestion des concessions funéraires | 2 : Significative | 2 : Limité | 4 : Limité |
| B-BILLET-T : perte de Traçabilité sur Billetterie en ligne | 1 : Minime | 2 : Limité | 3 : Faible |
| I-LOISIR-T : perte de Traçabilité sur Inscription aux centres de loisir | 1 : Minime | 2 : Limité | 3 : Faible |

**Tableau 21 – Classement des risques résiduels par niveau de risque**

| | | | | | |
|---|---|---|---|---|---|
| Vraisemblance | 4 : Maximale | | | | |
| | 3 : Forte | | | | |
| | 2 : Significative | | B-BILLET-C<br>I-LOISIR-D<br>I-LOISIR-I<br>I-LOISIR-C<br>E-CLOUD-I<br>E-PROC-C<br>M-MAIRE-I<br>M-MAIRE-C<br>C-FUNER-C | | |
| | 1 : Minime | | B-BILLET-T<br>I-LOISIR-T | | EXTRANET-T |
| | | 1 : Négligeable | 2 : Limité | 3 : Important | 4 : Critique |
| | | Gravité d'impact | | | |

**Figure 2 – Cartographie des risques résiduels**

Le diagramme suivant représente les niveaux de risque intrinsèque, actuels et résiduels pour chacun des évènements redoutés.

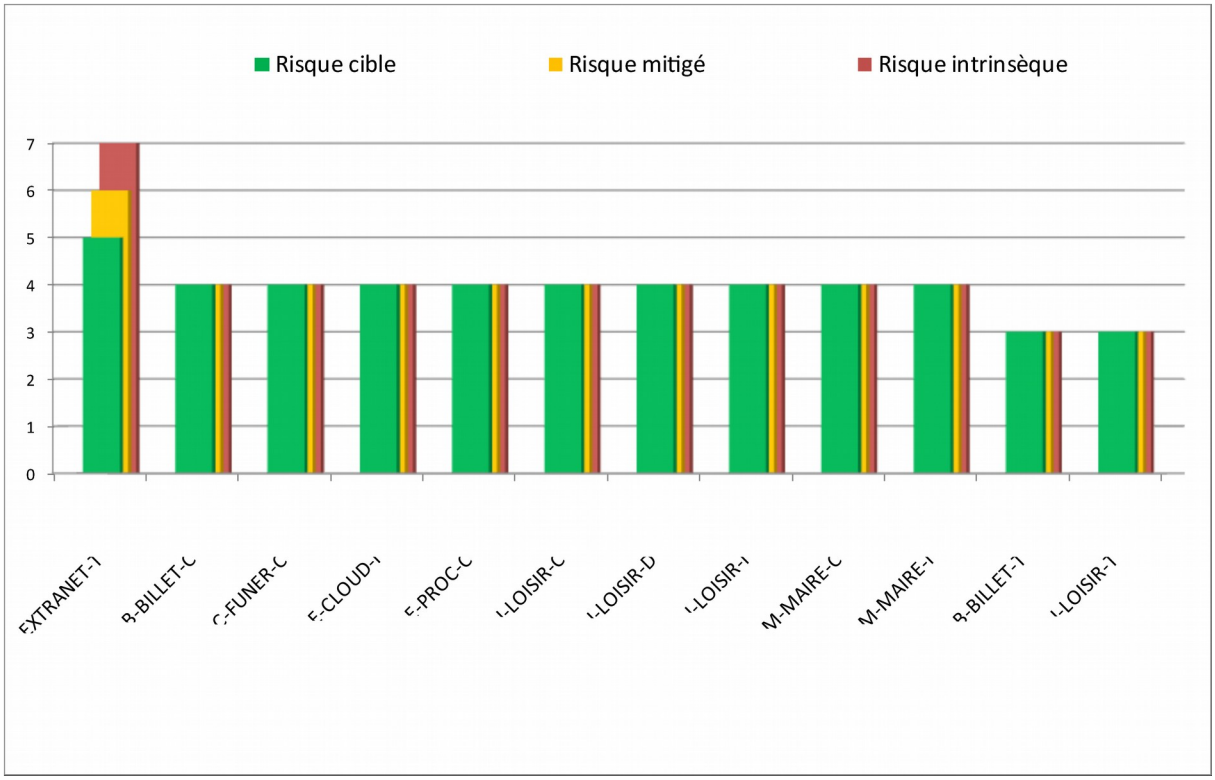



**Figure 3 – Représentation graphique des risques intrinsèque, actuels et résiduels**

# 2.ANNEXES

## 2.1.Biens support et liens avec les biens essentiels

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M-ACC | Mairie | LOC-ACC | Oui | Contrôle d'accès aux locaux mairie | | | x | x | x | x | x | x | x | x | x |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M-SRV | Mairie | LOC-SRV | Oui | Service locaux mairie (EDF, Clim, ...) | | | x | x | x | x | x | x | x | x | x |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M-ADM | Mairie | ORG-PER | Oui | Administrateur mairie | | | x | x | x | x | x | x | x | x | x |
| M-SPPIP | Mairie | SYS-LOG-APP | Oui | SPIP | | ASPIP : Mr DIJOUX | x | x | x | x | x | x | | | x |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M-APPLI | Mairie | SYS-LOG-APP | Oui | Applications et progiciel métier | | | | | | | | | x | | |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M-CLOUD | Mairie | SYS-LOG-APP | Oui | Partage d'espace cloud | | RINFRA : Mr AMADELLI | | | | | | | | x | |
| M-MYSQL | Mairie | SYS-LOG-BDD | Oui | MySQL | | ASPIP : Mr DIJOUX | | | x | x | x | x | | x | x |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M-SQLS | Mairie | SYS-LOG-BDD | Oui | Microsoft SQL server | | ASQL : Mr ANDRE JEWSKI | x | x | | x | | | x | | x |
| M-ORA | Mairie | SYS-LOG-BDD | Oui | Oracle | | AORA : Mr HOUE | | | | | | x | x | | |
| M-EXP | Mairie | SYS-LOG-EXP | Oui | Windows | | RINFRA : Mr AMADELLI | x | x | x | x | x | x | | | x |
| M-MDW | Mairie | SYS-LOG-MDW | Oui | IIS | | ASQL : Mr ANDRE JEWSKI | x | x | x | x | x | x | | | x |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M-COM | Mairie | SYS-MAT-COM | Oui | Switch réseau local | | RINFRA : Mr AMADELLI | x | x | x | x | x | x | x | x | x |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M-VPN | Mairie | SYS-MAT-COM | Oui | Concentrateur VPN SSL | | RINFRA : Mr AMADELLI | | | | | | | x | | |
| M-SRV | Mairie | SYS-MAT-SRV | Oui | Serveur (virtuel) | | RINFRA : Mr AMADELLI | x | x | x | x | x | x | x | x | x |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| M-SUP | Mairie | SYS-MAT-SUP | Oui | Baie de disques | | RINFRA : Mr AMADELLI | x | x | x | x | x | x | x | x | x |
| M-RINT | Mairie | SYS-RSX-RSD | Oui | Accès Internet mairie | | RINFRA : Mr AMADELLI | x | x | x | x | x | x | x | x | x |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E-ACC | Neyrial | LOC-ACC | Non | Contrôle d'accès aux locaux prestataire | Hors périmètre de l'analyse | | | | | | | | | | |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E-SRV | Neyrial | LOC-SRV | Non | Service locaux prestataire (EDF, Clim, | Hors périmètre de l'analyse | | | | | | | | | | |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E-ADM | Neyrial | ORG-PER | Non | Administrateur du prestataire | Hors périmètre de l'analyse | | | | | | | | | | |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E-SPIP | Neyrial | SYS-LOG-APP | Oui | Portail SPIP | | ASPIP : Mr DIJOUX | x | x | x | x | x | x | | | x |
| E-APHP | Neyrial | SYS-LOG-APP | Oui | Applications PHP | | ASQL : Mr ANDREJEWSKI | x | x | | x | | | | | x |
| E-BDD | Neyrial | SYS-LOG-BDD | Oui | MySQL | | ASPIP : Mr DIJOUX | x | x | x | x | x | x | | | x |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E-EXP | Neyrial | SYS-LOG-EXP | Non | Linux Debian | Hors périmètre de l'analyse | | | | | | | | | | |
| E-MDW | Neyrial | SYS-LOG-MDW | Oui | Apache | | ASPIP : Mr DIJOUX | x | x | x | x | x | x | | | x |
| E-COM | Neyrial | SYS-MAT-COM | Non | Switch réseau local | Hors périmètre de l'analyse | | | | | | | | | | |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E-SRV | Neyrial | SYS-MAT-SRV | Non | Serveur (virtuel) | Hors périmètre de l'analyse | | | | | | | | | | |
| E-SUP | Neyrial | SYS-MAT-SUP | Non | Baie de disques | Hors périmètre de l'analyse | | | | | | | | | | |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| E-INT | Neyrial | SYS-RSX-RSD | Oui | Accès Internet | | | x | x | x | x | x | x | | | x |

| Code | Site | Famille | Ret-enu | Bien | Commentaire | Propriétaire | S-ANOMA | C-EFTAG | A-CRISE | O-EMPLOI | B-BILLET | I-LOISIR | EXTRANET | E-CLOUD | E-PROC |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| R-EXM | Réseau | SYS-RSX-RSD | Oui | Lien entre le prestataire et la mairie | | RINFRA : Mr AMADELLI | x | x | x | x | x | x | | | x |

## 2.2.Mesures existantes

| Code | **Hypothèse ou mesure existante** | Familles de biens supports affectés | Rete-nue | Efficacité | D | I | C | T | Commentaire |
|---|---|---|---|---|---|---|---|---|---|
| MES-01 | Contrôle du canal de maintenance | SYS-MAT-COM : Relais de communication | Oui | 4 : Très efficace | | | | x | Pour les opérations de maintenance, il y a ouverture de canal à identifiant de session unique |
| MES-02 | Logs des accès VPN | SYS-MAT-COM : Relais de communication | Oui | 2 : Sensible | | | | x | Les accès VPN pour le personnel interne sont tracés |
| MES-03 | Profils d'accès pour les partenaires | SYS-MAT-COM : Relais de communication | Oui | 3 : Efficace | | | | x | Les accès VPN des partenaires ne se font qu'au travers du portail avec des accès définis par le profil (en https, SSH ou RDP) |

## 2.3.Evènements redoutés

| Code | **Evènement redouté** | Bien essentiel | Besoin sécurité | Impacts | Retenu | Gravité |
|---|---|---|---|---|---|---|
| EXTRANET-T | perte de Traçabilité sur Accès aux applications de la mairie d'après profil, en VPN SSL (mot de passe) | EXTRANET : Accès aux applications de la mairie d'après profil, en VPN SSL (mot de passe) | T=4 : Opposable | FON-MIS : 4 : Critique : Intrusion dans le SI | Oui | 4 : Critique |
| B-BILLET-C | perte de Confidentialité sur Billetterie en ligne | B-BILLET : Billetterie en ligne | C=3 : Confidentiel | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>DIV-JUR : 2 : Limité : Plainte d'usager avec recours | Oui | 2 : Limité |
| B-BILLET-T | perte de Traçabilité sur Billetterie en ligne | B-BILLET : Billetterie en ligne | T=3 : Essentielle | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>DIV-JUR : 2 : Limité : Plainte d'usager avec recours | Oui | 2 : Limité |
| I-LOISIR-D | perte de Disponibilité sur Inscription aux centres de loisir | I-LOISIR : Inscription aux centres de loisir | D=3 : Critique | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>FON-MIS : 2 : Limité : Difficulté de réserver une activité Espace Famille<br>DIV-NCF : 2 : Limité : Perte du label Qualiville | Oui | 2 : Limité |
| I-LOISIR-I | perte d'Intégrité sur Inscription aux centres de loisir | I-LOISIR : Inscription aux centres de loisir | I=3 : Maîtrisée | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>FON-MIS : 2 : Limité : Difficulté de réserver une activité Espace Famille<br>DIV-NCF : 2 : Limité : Perte du label Qualiville | Oui | 2 : Limité |
| I-LOISIR-C | perte de Confidentialité sur Inscription aux centres de loisir | I-LOISIR : Inscription aux centres de loisir | C=3 : Confidentiel | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>FON-MIS : 2 : Limité : Difficulté de réserver une activité Espace Famille<br>DIV-NCF : 2 : Limité : Perte du label Qualiville | Oui | 2 : Limité |

| Code | **Evènement redouté** | Bien essentiel | Besoin sécurité | Impacts | Retenu | Gravité |
|---|---|---|---|---|---|---|
| I-LOISIR-T | perte de Traçabilité sur Inscription aux centres de loisir | I-LOISIR : Inscription aux centres de loisir | T=3 : Essentielle | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>DIV-JUR : 2 : Limité : Plainte d'usager avec recours<br>FON-MIS : 2 : Limité : Difficulté de réserver une activité Espace Famille<br>DIV-NCF : 2 : Limité : Perte du label Qualiville | Oui | 2 : Limité |
| E-CLOUD-I | perte d'Intégrité sur Plateforme d'échange avec les fournisseurs | E-CLOUD : Plateforme d'échange avec les fournisseurs | I=3 : Maîtrisée | DIV-JUR : 2 : Limité : Plainte d'usager avec recours | Oui | 2 : Limité |
| E-PROC-C | perte de Confidentialité sur Formulaire électronique sans authentification | E-PROC : Formulaire électronique sans authentification | C=3 : Confidentiel | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>DIV-JUR : 2 : Limité : Plainte d'usager avec recours | Oui | 2 : Limité |
| M-MAIRE-I | perte d'Intégrité sur Ecrire au maire | M-MAIRE : Ecrire au maire | I=2 : Détectable | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>DIV-JUR : 2 : Limité : Plainte d'usager avec recours<br>BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Oui | 2 : Limité |
| M-MAIRE-C | perte de Confidentialité sur Ecrire au maire | M-MAIRE : Ecrire au maire | C=3 : Confidentiel | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>DIV-JUR : 2 : Limité : Plainte d'usager avec recours<br>BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Oui | 2 : Limité |
| S-ANOMA-D | perte de Disponibilité sur Signaler une anomalie sur espace public | S-ANOMA : Signaler une anomalie sur espace public | D=2 : Nécessaire | BNS-IMA : 1 : Négligeable : Le service est délaissé<br>BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Non | 1 : Négligeable |
| S-ANOMA-I | perte d'Intégrité sur Signaler une anomalie sur espace public | S-ANOMA : Signaler une anomalie sur espace public | I=2 : Détectable | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Non | 1 : Négligeable |

| Code | **Evènement redouté** | Bien essentiel | Besoin sécurité | Impacts | Retenu | Gravité |
|---|---|---|---|---|---|---|
| S-ANOMA-C | perte de Confidentialité sur Signaler une anomalie sur espace public | S-ANOMA : Signaler une anomalie sur espace public | C=2 : Restreint | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Non | 1 : Négligeable |
| S-ANOMA-T | perte de Traçabilité sur Signaler une anomalie sur espace public | S-ANOMA : Signaler une anomalie sur espace public | T=1 : Minimum | BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Non | 1 : Négligeable |
| C-EFTAG-D | perte de Disponibilité sur Demander l'effacement de tags | C-EFTAG : Demander l'effacement de tags | D=2 : Nécessaire | BNS-IMA : 1 : Négligeable : Le service est délaissé<br>BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Non | 1 : Négligeable |
| C-EFTAG-I | perte d'Intégrité sur Demander l'effacement de tags | C-EFTAG : Demander l'effacement de tags | I=2 : Détectable | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Non | 1 : Négligeable |
| C-EFTAG-C | perte de Confidentialité sur Demander l'effacement de tags | C-EFTAG : Demander l'effacement de tags | C=2 : Restreint | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Non | 1 : Négligeable |
| C-EFTAG-T | perte de Traçabilité sur Demander l'effacement de tags | C-EFTAG : Demander l'effacement de tags | T=1 : Minimum | BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Non | 1 : Négligeable |
| O-EMPLOI-D | perte de Disponibilité sur Consulter et postuler aux offres d'emploi | O-EMPLOI : Consulter et postuler aux offres d'emploi | D=2 : Nécessaire | BNS-IMA : 1 : Négligeable : Usagers mécontents | Non | 1 : Négligeable |
| O-EMPLOI-I | perte d'Intégrité sur Consulter et postuler aux offres d'emploi | O-EMPLOI : Consulter et postuler aux offres d'emploi | I=2 : Détectable | BNS-IMA : 1 : Négligeable : Usagers mécontents | Non | 1 : Négligeable |
| O-EMPLOI-C | perte de Confidentialité sur Consulter et postuler aux offres d'emploi | O-EMPLOI : Consulter et postuler aux offres d'emploi | C=3 : Confidentiel | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>DIV-JUR : 2 : Limité : Plainte d'usager avec recours | Non | 1 : Négligeable |
| O-EMPLOI-T | perte de Traçabilité sur Consulter et postuler aux offres d'emploi | O-EMPLOI : Consulter et postuler aux offres d'emploi | T=2 : Nécessaire | BNS-IMA : 1 : Négligeable : Usagers mécontents | Non | 1 : Négligeable |

| Code | **Evènement redouté** | Bien essentiel | Besoin sécurité | Impacts | Retenu | Gravité |
|---|---|---|---|---|---|---|
| B-BILLET-D | perte de Disponibilité sur Billetterie en ligne | B-BILLET : Billetterie en ligne | D=3 : Critique | BNS-IMA : 1 : Négligeable : Usagers mécontents | Non | 1 : Négligeable |
| B-BILLET-I | perte d'Intégrité sur Billetterie en ligne | B-BILLET : Billetterie en ligne | I=3 : Maîtrisée | BNS-IMA : 1 : Négligeable : Usagers mécontents | Non | 1 : Négligeable |
| EXTRANET-D | perte de Disponibilité sur Accès aux applications de la mairie d'après profil, en VPN SSL (mot de passe) | EXTRANET : Accès aux applications de la mairie d'après profil, en VPN SSL (mot de passe) | D=3 : Critique | BNS-IMA : 1 : Négligeable : Usagers mécontents | Non | 1 : Négligeable |
| E-CLOUD-D | perte de Disponibilité sur Plateforme d'échange avec les fournisseurs | E-CLOUD : Plateforme d'échange avec les fournisseurs | D=2 : Nécessaire | BNS-IMA : 1 : Négligeable : Usagers mécontents | Non | 1 : Négligeable |
| E-CLOUD-T | perte de Traçabilité sur Plateforme d'échange avec les fournisseurs | E-CLOUD : Plateforme d'échange avec les fournisseurs | T=3 : Essentielle | BNS-IMA : 1 : Négligeable : Usagers mécontents | Non | 1 : Négligeable |
| E-PROC-D | perte de Disponibilité sur Formulaire électronique sans authentification | E-PROC : Formulaire électronique sans authentification | D=3 : Critique | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>BNS-IMA : 1 : Négligeable : Le service est délaissé | Non | 1 : Négligeable |
| E-PROC-I | perte d'Intégrité sur Formulaire électronique sans authentification | E-PROC : Formulaire électronique sans authentification | I=2 : Détectable | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>FON-MIS : 1 : Négligeable : Encombrement des services | Non | 1 : Négligeable |
| E-PROC-T | perte de Traçabilité sur Formulaire électronique sans authentification | E-PROC : Formulaire électronique sans authentification | T=2 : Nécessaire | BNS-IMA : 1 : Négligeable : Usagers mécontents | Non | 1 : Négligeable |
| C-FUNER-D | perte de Disponibilité sur Gestion des concessions funéraires | C-FUNER : Gestion des concessions funéraires | D=3 : Critique | BNS-IMA : 1 : Négligeable : Le service est délaissé<br>FON-MIS : 1 : Négligeable : Encombrement des services | Non | 1 : Négligeable |
| C-FUNER-I | perte d'Intégrité sur Gestion des concessions funéraires | C-FUNER : Gestion des concessions funéraires | I=3 : Maîtrisée | BNS-IMA : 1 : Négligeable : Le service est délaissé | Non | 1 : Négligeable |

| Code | **Evènement redouté** | Bien essentiel | Besoin sécurité | Impacts | Retenu | Gravité |
|---|---|---|---|---|---|---|
| C-FUNER-C | perte de Confidentialité sur Gestion des concessions funéraires | C-FUNER : Gestion des concessions funéraires | C=2 : Restreint | BNS-IMA : 1 : Négligeable : Usagers mécontents<br>DIV-JUR : 2 : Limité : Plainte d'usager avec recours | Oui | 2 : Limité |
| M-MAIRE-D | perte de Disponibilité sur Ecrire au maire | M-MAIRE : Ecrire au maire | D=3 : Critique | BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Non | 1 : Négligeable |
| M-MAIRE-T | perte de Traçabilité sur Ecrire au maire | M-MAIRE : Ecrire au maire | T=3 : Essentielle | BNS-IMA : 1 : Négligeable : Perte de confiance dans les engagements politiques | Non | 1 : Négligeable |
| C-FUNER-T | perte de Traçabilité sur Gestion des concessions funéraires | C-FUNER : Gestion des concessions funéraires | T=1 : Minimum | FON-MIS : 1 : Négligeable : Perte de temps dans la recherche d'un acteur | Non | 1 : Négligeable |

## 2.4.Vulnérabilités

| Code | **Vulnérabilité** et niveau d'exposition | Retenue | Justification si non retenue |
|---|---|---|---|
| LOG-01 | Possibilité de détournement d'usage | Oui | |
| LOG-02 | Faiblesse de la protection d'accès aux fonctions | Oui | |
| LOG-03 | Faiblesse de la protection d'accès aux données | Oui | |
| LOG-07 | Faiblesse du contrôle des volumes entrés | Oui | |
| LOG-09 | Possibilité d'effacement de programme | Oui | |
| LOG-10 | Complexité d'administration | Oui | |
| LOG-13 | Mauvaise maîtrise du développement ou du paramétrage | Oui | |
| LOG-16 | Manque d'adaptation à l'évolution des systèmes | Oui | |
| MAT-01 | Possibilité de détournement d'usage | Oui | |
| MAT-04 | Insuffisance de la capacité de traitement | Oui | |
| MAT-05 | Insuffisance de la capacité de stockage | Oui | |
| PER-07 | Facilité de rupture du lien contractuel | Oui | |
| PER-09 | Manque de ressource pour les tâches assignées | Oui | |
| PHY-01 | Insuffisance ou défaut d'alimentation électrique | Oui | |
| PHY-02 | Faiblesse du contrôle d'accès | Oui | |
| PHY-03 | Insuffisance ou panne de climatisation | Oui | |
| PHY-04 | Insuffisance de la protection incendie | Oui | |
| PHY-06 | Insuffisance de la protection physique du site | Oui | |
| RSX-01 | Possibilité de modifier les flux de données | Oui | HTTPS partout |
| RSX-04 | Insuffisance de la capacité de transmission | Oui | QOS + Double adduction |
| RSX-09 | Faiblesse du chiffrement des transmissions | Oui | HTTPS partout |
| CAN-01 | Possibilité de modification des flux | Non | Hors périmètre des télé-services |
| CAN-02 | Unicité du circuit organisationnel | Non | Hors périmètre des télé-services |
| CAN-03 | Possibilité de modification du circuit organisationnel | Non | Hors périmètre des télé-services |
| CAN-04 | Possibilité d'écoute passive | Non | Hors périmètre des télé-services |
| CAN-05 | L'utilité du canal n'est pas reconnue | Non | Hors périmètre des télé-services |
| LOG-04 | Faiblesse de la protection d'accès au code source | Non | |
| LOG-05 | Possibilité de comprendre le fonctionnement | Non | |
| LOG-06 | Faiblesse du contrôle des données entrées | Non | Contrôles de type |
| LOG-08 | Faiblesse du contrôle des traitements | Non | |
| LOG-11 | Absence de sauvegarde des exécutables | Non | Exécutables sauvegardés |
| LOG-12 | Facilité de modification des sources ou des fonctions | Non | |
| LOG-14 | Manque d'adaptation au besoin métier | Non | |
| LOG-15 | Licence caduque ou cédée | Non | |
| MAT-02 | Emission de signaux compromettants | Non | |
| MAT-03 | Observable à distance | Non | |
| MAT-06 | Mauvaise qualité des composants | Non | |
| MAT-07 | Manque d'adaptation aux conditions d'utilisation | Non | |
| MAT-08 | Possibilité de connecter des périphériques | Non | Serveurs virtuels sans USB |
| MAT-09 | Possibilité de désactiver des composants matériels | Non | |
| MAT-10 | Attractivité du composant | Non | |

| Code | **Vulnérabilité** et niveau d'exposition | Retenue | Justification si non retenue |
|---|---|---|---|
| MAT-11 | Bon rapport valeur / encombrement | Non | |
| PAP-01 | Possibilité de détournement d'usage | Non | Hors périmètre des télé-services |
| PAP-02 | Possibilité de falsification | Non | Hors périmètre des télé-services |
| PAP-03 | Manque de protection des supports classifiés | Non | Hors périmètre des télé-services |
| PAP-04 | Possibilité d'altération, destruction ou perte | Non | Hors périmètre des télé-services |
| PER-01 | Personne distraite ou dissipée | Non | |
| PER-02 | Personne peu discrète, routinière, influençable | Non | |
| PER-03 | Manque de redondance des compétences | Non | |
| PER-04 | Profils inadaptés aux exigences du métier | Non | |
| PER-05 | Personne résistante au changement | Non | |
| PER-06 | Faible satisfaction des besoins personnels | Non | |
| PER-08 | Manque de loyauté d'une personne | Non | |
| PHY-05 | Possibilité de rupture de la fourniture eau | Non | |
| RSX-02 | Emission de rayonnements interprétables | Non | |
| RSX-03 | Possibilité d'écoute passive | Non | |
| RSX-05 | Fragilité du support physique | Non | Virtualisé |
| RSX-06 | Mauvaise protection contre les rayonnements | Non | |
| RSX-07 | Possibilité de détruire ou voler un support | Non | Pas de support amovible |
| RSX-08 | Unicité du canal de transmission | Non | Double adduction par 2 opérateurs différents |
| RSX-10 | Câble techniquement inadapté | Non | |

## 2.5.Menaces

| Code | **Menaces** | D | I | C | T | Retenue |
|---|---|---|---|---|---|---|
| LOG-DET | Suppression de tout ou partie d'un logiciel | X | | | | Oui |
| LOG-MOD | Modification d'un logiciel | X | X | X | | Oui |
| MAT-DEP | Dépassement des limites de fonctionnement d'un matériel | X | | | | Oui |
| MAT-USG | Détournement de l'usage prévu d'un matériel | X | X | X | X | Oui |
| PER-DEP | Surcharge des capacités d'une personne | X | X | | | Oui |
| PER-PTE | Départ d'une personne | X | | X | | Oui |
| PHY-DET | Détérioration d'un local ou d'un service | X | | | | Oui |
| RSX-DEP | Saturation d'un canal informatique ou de téléphonie | X | | | | Oui |
| RSX-DET | Dégradation d'un canal informatique ou de téléphonie | X | | | | Oui |
| RSX-ESP | Écoute passive d'un canal informatique ou de téléphonie | | | | X | Oui |
| RSX-PTE | Disparition d'un canal informatique ou de téléphonie | X | | | | Oui |
| CAN-DEP | Saturation d'un canal interpersonnel | X | | | | Non |
| CAN-DET | Dégradation d'un canal interpersonnel | X | | | | Non |
| CAN-ESP | Espionnage d'un canal interpersonnel | | | X | | Non |
| CAN-MOD | Modification d'un canal interpersonnel | X | | | | Non |
| CAN-PTE | Disparition d'un canal interpersonnel | X | | | | Non |
| CAN-USG | Manipulation via un canal interpersonnel | X | X | | | Non |
| LOG-DEP | Dépassement des limites d'un logiciel | X | | | | Non |
| LOG-ESP | Analyse d'un logiciel | | | X | | Non |
| LOG-PTE | Perte d'un logiciel | X | | X | | Non |
| LOG-USG | Détournement de l'usage prévu d'un logiciel | X | X | X | | Non |
| MAT-DET | Détérioration d'un matériel | X | X | X | | Non |
| MAT-ESP | Espionnage d'un matériel | | | X | | Non |
| MAT-MOD | Modification d'un matériel | X | X | X | | Non |
| MAT-PTE | Perte ou vol d'un matériel | X | | X | | Non |
| PAP-DET | Détérioration d'un support papier | X | | | | Non |
| PAP-ESP | Espionnage d'un support papier | | | X | | Non |
| PAP-PTE | Perte ou vol d'un support papier | X | | X | | Non |
| PAP-USG | Détournement de l'usage prévu d'un support papier | X | X | | | Non |
| PER-DET | Dégradation d'une personne | X | | | | Non |
| PER-ESP | Espionnage d'une personne à distance | | | X | | Non |
| PER-MOD | Influence sur une personne | | X | X | | Non |
| PER-USG | Dissipation de l'activité d'une personne | X | | | | Non |
| PHY-DEG | Dégradation d'un local ou d'un service | X | | | | Non |
| PHY-ESP | Espionnage d'un local ou d'un service | X | X | X | | Non |
| PHY-USG | Détournement d'usage d'un local ou d'un service | X | | | | Non |
| RSX-MOD | Modification d'un canal informatique ou de téléphonie | X | | | | Non |
| RSX-USG | Attaque du milieu sur un canal informatique ou de téléphonie | X | X | | | Non |

## 2.6.Mesures restant à prendre

| Code | **Mesure à prendre** | Famille de Bien support | Biens supports | Thème ISO 27002 | Note ISO | Prev | Prot | Rec | Efficacité estimée | D | I | C | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Contractualiser les relations avec | | | | | | | | 4 | | | | |

| Code | **Mesure à prendre** | Famille de Bien support | Biens supports | Thème ISO 27002 | Note ISO | Prev | Prot | Rec | Efficacité estimée | D | I | C | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Imposer des mots de passe c | | | | | | | | 4 | | | | |

| Code | **Mesure à prendre** | Famille de Bien support | Biens supports | Thème ISO 27002 | Note ISO | Prev | Prot | Rec | Efficacité estimée | D | I | C | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A-001 | Authentification forte pour les utili | SYS-MAT-COM : Relais de communication | M-VPN : SYS-MAT-COM : Concentrateur VPN SSL | | | | x | | 4 : Très ef | | | | X |

| Code | **Mesure à prendre** | Famille de Bien support | Biens supports | Thème ISO 27002 | Note ISO | Prev | Prot | Rec | Efficacité estimée | D | I | C | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A-002 | Ouverture dynamique du canal | SYS-MAT-COM : Relais de communication | M-VPN : SYS-MAT-COM : Concentrateur VPN SSL | | | | x | | 4 : Très eff | | | | x |

| Code | **Mesure à prendre** | Famille de Bien support | Biens supports | Thème ISO 27002 | Note ISO | Prev | Prot | Rec | Efficacité estimée | D | I | C | T |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A-004 | Formaliser les procédures d'expl | SYS-MAT-SRV : Serveur<br>SYS-MAT-COM : Relais de communication<br>SYS-MAT-SUP : Support électronique<br>SYS-LOG-APP : Application<br>SYS-LOG-BDD : Sys Gest base de données<br>SYS-LOG-MDW : Intergiciel | | | | x | | | 2 : Sens | X | | | |