PREMIER MINISTRE
Secrétariat général de la défense et de la sécurité nationale
Agence nationale de la sécurité des systèmes d'information
Sous-direction assistance, conseil et expertise
Bureau assistance et conseil

Expression des Besoins et Identification des Objectifs de Sécurité

EBIOS

ÉTUDE DE CAS @RCHIMED

Version du 25 janvier 2010

51 boulevard de La Tour-Maubourg - 75700 PARIS 07 SP - Tél 01 71 75 84 65 - Fax 01 71 75 84 90

Historique des modifications

Date	Objet de la modification	Statut
06/09/2000	Création de l'étude de cas selon EBIOSv1	Validé
16/07/2004	Révision de l'étude de cas selon EBIOSv2	Validé
25/01/2010	Révision de l'étude de cas selon la dernière évolution d'EBIOS	Validé

Table des matières

Avant-propos

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) élabore et tient à jour un important référentiel méthodologique destiné à aider les organismes du secteur public et du secteur privé à gérer la sécurité de leurs systèmes d'informations. Ce référentiel est composé de méthodes, de meilleures pratiques et de logiciels, diffusés gratuitement sur son site Internet (http://www.ssi.gouv.fr).

Le Club EBIOS est une association indépendante à but non lucratif (Loi 1901), composée d'experts individuels et d'organismes. Il regroupe une communauté de membres du secteur public et du secteur privé, français et européens. Il supporte et enrichit le référentiel de gestion des risques français depuis 2003, en collaboration avec l'ANSSI. Le Club organise des réunions périodiques pour favoriser les échanges d'expériences, l'homogénéisation des pratiques et la satisfaction des besoins des usagers. Il constitue également un espace pour définir des positions et exercer un rôle d'influence dans les débats nationaux et internationaux.

Ce document a été réalisé par le bureau assistance et conseil de l'ANSSI, avec la collaboration du Club EBIOS. La communauté des utilisateurs d'EBIOS enrichit régulièrement le référentiel complémentaire à ce document (techniques de mise en œuvre, bases de connaissances, guides d'utilisations spécifiques de la méthode, documents relatifs à la communication, à la formation, à la certification, logiciels…).

Introduction

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

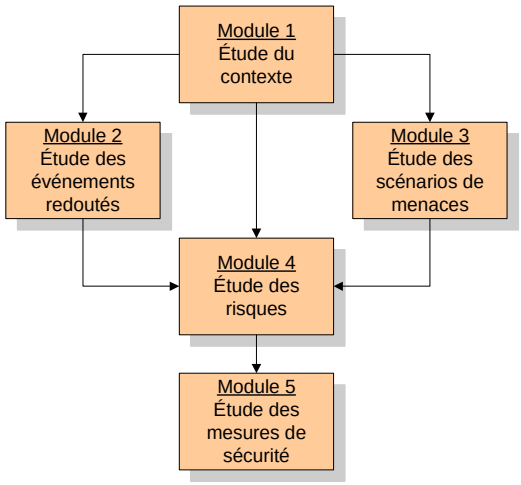

Figure 1 - Étapes de la démarche EBIOS

La première partie du document constitue le dossier de présentation de la société @RCHIMED. La seconde partie décrit l'étude de sécurité. La dernière partie est constituée des livrables produits.

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

1 Dossier de présentation de la société @RCHIMED

Ce chapitre présente les informations relatives à la société @RCHIMED. Elles ont été collectées suite à un entretien avec les responsables de l'entreprise. Des compléments d'informations pourront être demandés en cours d'étude.

Présentation générale de la société

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

Prestation fournie

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

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

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

Par ailleurs, elle a créé son site Internet sur lequel sont présentés les informations concernant la société et des exemples de devis et de maquettes virtuelles.

Clientèle

Cette entreprise compte de nombreux clients, privés ou publics, ainsi que plusieurs professionnels du bâtiment.

Les statistiques menées depuis 3 ans montrent des périodes de pointe situées entre octobre et mai et que la conjoncture générale du domaine de l'architecture est bonne.

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

Structure de la société

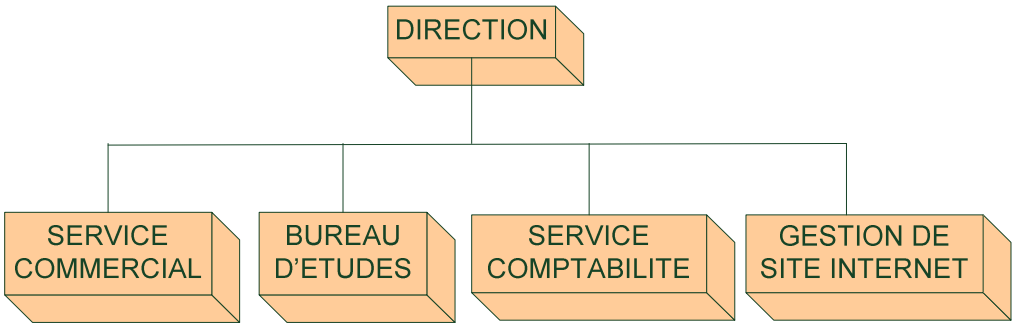

Figure 2 - Organigramme de la société

La direction

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

Le service commercial

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

Seul, le service commercial est habilité à traiter avec l'extérieur, il est donc garant de l'image de marque de l'entreprise. Il échange fréquemment des informations avec le bureau d'études (création des plans, création des maquettes virtuelles…), avec la comptabilité (création des devis, coûts…) et avec l'extérieur (cahier des charges, plans, devis; maquettes virtuelles, éléments techniques pour les fournisseurs…)

Le bureau d'études

Il est composé de 4 ingénieurs et 3 techniciens supérieurs et réalise les activités suivantes :

- élaborer des plans d'exécution destinés aux professionnels ;
- élaborer des maquettes virtuelles attrayante destinés aux clients ;
- établir des calculs de résistances de structures et de matériaux.

Le service comptabilité

Le service chargé de toutes les finances de la société est composé d'un seul comptable. Il traite notamment avec la Direction départementale de l'équipement (DDE) pour les acceptations de permis de construire et s'occupe également de tous les contentieux.

Le service de gestion de site Internet

Il est composé d'un administrateur chargé de mettre à jour le site Internet de la société.

Système informatique

Matériel

L'informatique de la société est reliée par un réseau Wifi et le bureau d'études dispose d'un réseau local de type Ethernet. Le site Internet est hébergé sur un serveur externe. Le bureau d'étude possède 7 ordinateurs, le service commercial 2 ordinateurs portables, le service comptabilité 1 ordinateur, et le service de gestion de site Internet 1 ordinateur.

Logiciels

Le cabinet a acquis les logiciels ARC+ pour le maquettage virtuel, SIFRA pour le travail à partir de tablettes graphiques et SPOT pour les calculs de résistance des matériaux. Cet investissement nécessaire a représenté un effort financier important (de l'ordre de 450 000 €). Le bureau d'études possède également un outil de présentation assisté par ordinateur (PAO) appelé Pagemaker. Tous les services sont équipés d'une suite bureautique. Les ordinateurs du bureau d'étude sont équipés de MAC OS X, le reste du cabinet est équipé de Windows® XP.

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

Schéma général du système

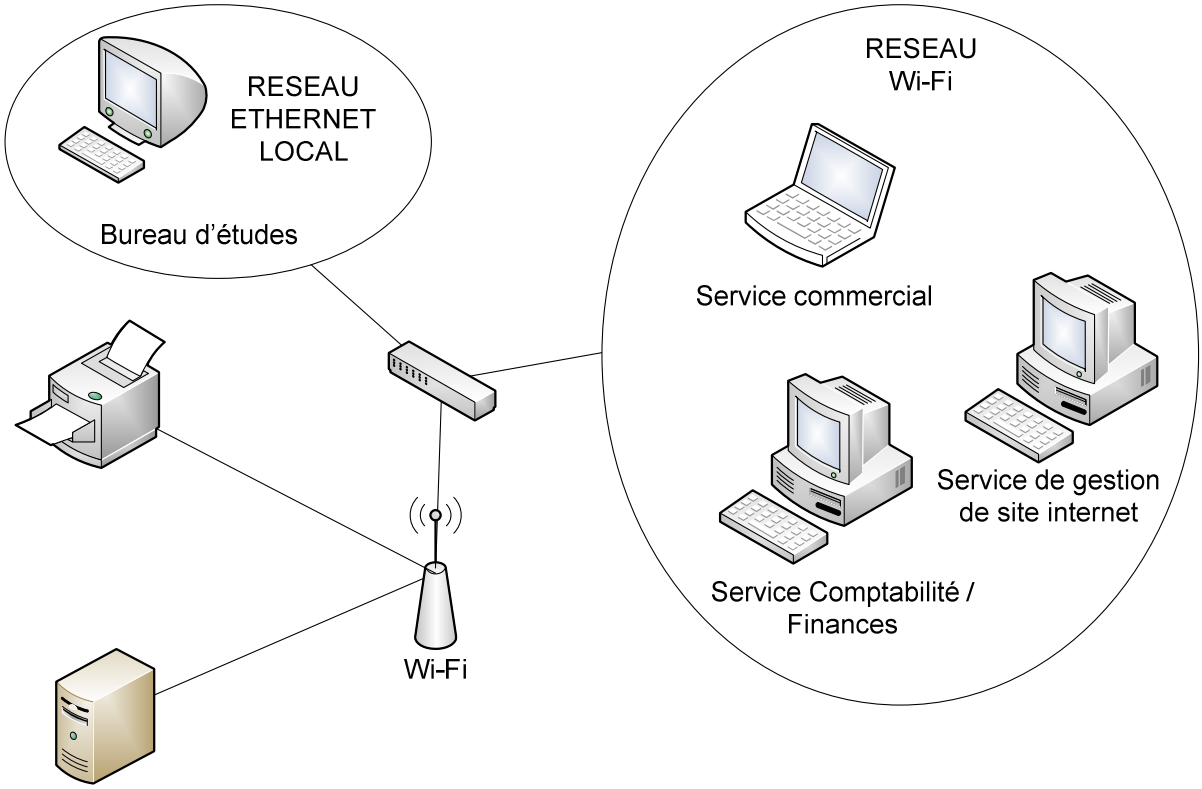

Figure 3 - Schéma général du système

Éléments de contexte

Sécurité générale

Les informations suivantes ont pu être recueillies au cours des entretiens avec la direction et de la visite des locaux d'@RCHIMED :

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

Sécurité du système d'information

Il n'y a pas de principes généraux, ni de politique de sécurité, seulement les quelques règles suivantes :

- le contrôle d'accès se fait par identifiant /mot de passe ;
- principe de sauvegarde de tout fichier ;
- chaque ingénieur est responsable du fichier qu'il traite, les fichiers sont sauvegardés sur des disques USB stockés dans une armoire fermant à clé, située dans le bureau d'études ;
- parallèlement, les documents papiers sont rangés dans une armoire forte du service commercial ;
- en ce qui concerne la maintenance, un contrat a été établi avec les fournisseurs de logiciels avec intervention sous 4 heures.

Conjoncture

La mise en réseau des systèmes informatiques s'est effectuée avec succès et a permis de réduire encore plus les délais de réalisation des travaux. L'entreprise doit maintenant répondre au souhait de la majorité des clients qui est de correspondre directement avec le bureau d'étude via Internet pour transmettre tous les types de documents (dossiers techniques, devis, appel d'offre, messages...).

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

D'autre part, de plus en plus de contrats pour lesquels @ARCHIMED souhaite se positionner sont conditionné par la capacité du cabinet à assurer la confidentialité relative aux aspects techniques du projet. Par exemple, L'appel d'offre pour la rénovation de certaines installations de la marine nationale de l'arsenal de Toulon entre dans ce cadre.

Compte tenu de son volume et de sa disposition, la société travaille de façon très ouverte. Cependant, les experts du bureau d'études sont les seuls à pouvoir accéder aux logiciels les plus performants de conception et de maquettage. Ces experts ont par ailleurs bénéficié d'une formation à la manipulation de ces outils. Chacun est conscient de ces responsabilités financières, civiles et pénales associées à l'usage des informations qu'il manipule : dossier client, données nominatives…

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

2 Étude des risques

Cette étude, réalisée à l'aide de la méthode EBIOS, fera l'objet d'un document interne, maintenu à jour par le responsable SSI. Il s'agit davantage d'un document de travail que d'un livrable. En effet, son contenu est nécessaire à la réalisation de l'étude et à l'élaboration des différents livrables qui pourront communiqués par la suite. Mais il n'a de réel intérêt, dans son fond et dans sa forme, que pour le responsable SSI.

Module 1 – Étude du contexte

Le cadre de la gestion des risques

L'objectif de l'étude : gérer les risques SSI sur le long terme et élaborer une politique

Le Directeur de la société @RCHIMED souhaite que les risques de sécurité de l'information qui pourraient empêcher l'organisme d'atteindre ses objectifs soient gérés, et ce, de manière continue, afin d'être au plus proche d'une réalité en mouvement.

Une politique de sécurité de l'information doit ainsi être produite, appliquée et contrôlée.

Par ailleurs, il n'exclut pas l'idée de faire certifier à terme les principales activités du cabinet selon l'ISO 27001 et reconnaît l'intérêt d'exploiter des meilleures pratiques reconnues internationalement (ISO 27002). Par conséquent, une déclaration d'applicabilité devrait être produite ultérieurement.

Le plan d'action : une réflexion sur 15 jours qui requiert la participation de tous

Pour ce faire, le cabinet @RCHIMED prévoit la structure de travail suivante :

Activités d'EBIOS	Directeur	Directeur adjoint	Comité de suivi	Secrétariat	Service commercial	Bureau d'études	Service comptabilité	Documents à produire en plus de l'étude des risques	Consignes particulières	Ressources estimées (en h.j)	Durée (en jours)
Activité 1.1 – Définir le cadre de la gestion des risques		R	C	I	I	I	I			2	2
Activité 1.2 – Préparer les métriques		R	C	I	I	I	I		Vérifier l'uniformité de la compréhension	2	2
Activité 1.3 – Identifier les biens	A	R	C	C	C	C	I	Note de cadrage	Ne pas trop détailler	6	2
Activité 2.1 – Apprécier les événements redoutés		R	C	C	C	C	I		Utiliser les bases génériques	6	2
Activité 3.1 – Apprécier les scénarios de menaces		R	C	C	C	C	I		Utiliser les bases génériques	6	2
Activité 4.1 – Apprécier les risques		R	C	I	I	I	I			1	1
Activité 4.2 – Identifier les objectifs de sécurité	A	R	C	I	I	I	I	Note de stratégie		2	1
Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre	A	R	C	C	C	C	I	Politique de sécurité de l'information		15	3
Activité 5.2 – Mettre en œuvre les mesures de sécurité	A	R	I	C	C	C	I	Homologation	Cette activité ne sera réalisée de suite	0	0

Légende : R = Réalisation ; A = Approbation ; C = Consultation ; I = Information

L'organisme étudié : la société @RCHIMED

Il s'agit d'une PME toulonnaise constituée d'une douzaine de personnes. C'est un bureau d'ingénierie en architecture qui réalise des plans d'usines et d'immeubles. Sa vocation principale est de vendre des services pour les professionnels du bâtiment.

@RCHIMED compte de nombreux clients, privés ou publics, ainsi que quelques professionnels du bâtiment.

Son capital s'élève à xxxxx € et son chiffre d'affaires à yyyyy €.
Ses missions consistent principalement à élaborer des projets architecturaux, ainsi que des calculs de structures et la création de plans techniques.
Ses valeurs sont la réactivité, la précision des travaux, la créativité architecturale et la communication.
Les principaux métiers représentés sont l'architecture et l'ingénierie du bâtiment.
Sa structure organisationnelle est fonctionnelle avec une direction, un service commercial, un bureau d'études, un service comptabilité et un service de gestion de site internet.
Ses axes stratégiques sont d'une part l'utilisation des nouvelles technologies (Internet, Intranet) dans un but d'ouverture vers l'extérieur et d'optimisation des moyens, et d'autre part la consolidation de l'image de marque (protection des projets sensibles).

Ses principaux processus métiers sont les suivants :

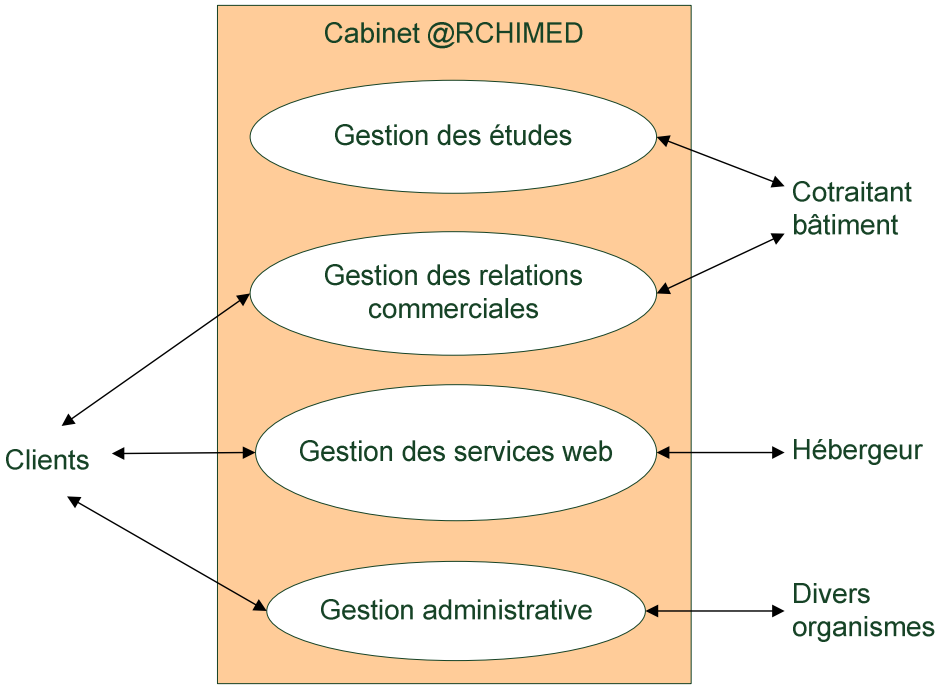

Figure 4 - Les principaux processus métiers de la société

Plusieurs éléments de conjoncture ont été identifiés :

- la mise en réseau des systèmes informatiques s'est effectuée avec succès et a permis de réduire encore plus les délais de réalisation des travaux ;
- l'entreprise a dernièrement perdu un marché : la rénovation de la mairie de Draguignan. Lors de la présentation des projets, il est apparu de curieuses similitudes entre la maquette virtuelle d'@RCHIMED et la proposition d'un concurrent de Nice. Le directeur d'@RCHIMED soupçonne une compromission du projet qu'il avait présenté. Il a maintenant des craintes sur la confidentialité de certains projets ;
- l'arsenal de Toulon semble vouloir rénover certaines installations servant à la maintenance des bâtiments de la marine nationale. @RCHIMED souhaiterait pouvoir se présenter à d'éventuels appels d'offres ;
- une rude concurrence, dépendant des appels d'offres, s'exerce dans le secteur ;
- seule une crise très grave dans le bâtiment pourrait affecter le fonctionnement du cabinet d'architecture.

Une gestion des risques intégrée

Le risque est défini comme un "scénario, avec un niveau donné, combinant un événement redouté par @RCHIMED sur son activité, et un ou plusieurs scénarios de menaces. Son niveau correspond à l'estimation de sa vraisemblance et de sa gravité".

En matière de gestion des risques, les rôles et responsabilités sont les suivants :

- le Directeur d'@RCHIMED est pleinement responsable des risques pesant sur sa société ;
- le Directeur adjoint a été mandaté pour animer la gestion des risques de sécurité de l'information ; il est ainsi responsable de la réalisation des études de risques ;
- un comité de suivi, composé d'un membre de chaque service et présidé par le Directeur adjoint, réalisera la première étude de risques et se réunira ensuite tous les six mois afin de faire le point sur les évolutions à apporter à la gestion des risques de sécurité de l'information.

Les interfaces de la gestion des risques sont les suivantes :

- la gestion des risques de sécurité de l'information est partie intégrante de la gestion d'@RCHIMED ; à ce titre, ses résultats sont pris en compte dans la stratégie de la société ;
- l'ensemble de la société est concerné par la gestion des risques de sécurité de l'information, tant pour apprécier les risques que pour appliquer et faire appliquer des mesures de sécurité.

Le sujet de l'étude : le cœur de métier d'@RCHIMED

Le choix du périmètre d'étude s'est porté sur le sous-ensemble du système d'information du cabinet @RCHIMED correspondant à son cœur de métier :

- gestion des relations commerciales (gestion des devis, projets…) ;
- gestion des études (calculs de structure, plans techniques, visualisations 3D…) ;
- gestion des services web (nom de domaine, site Internet, courrier électronique…).

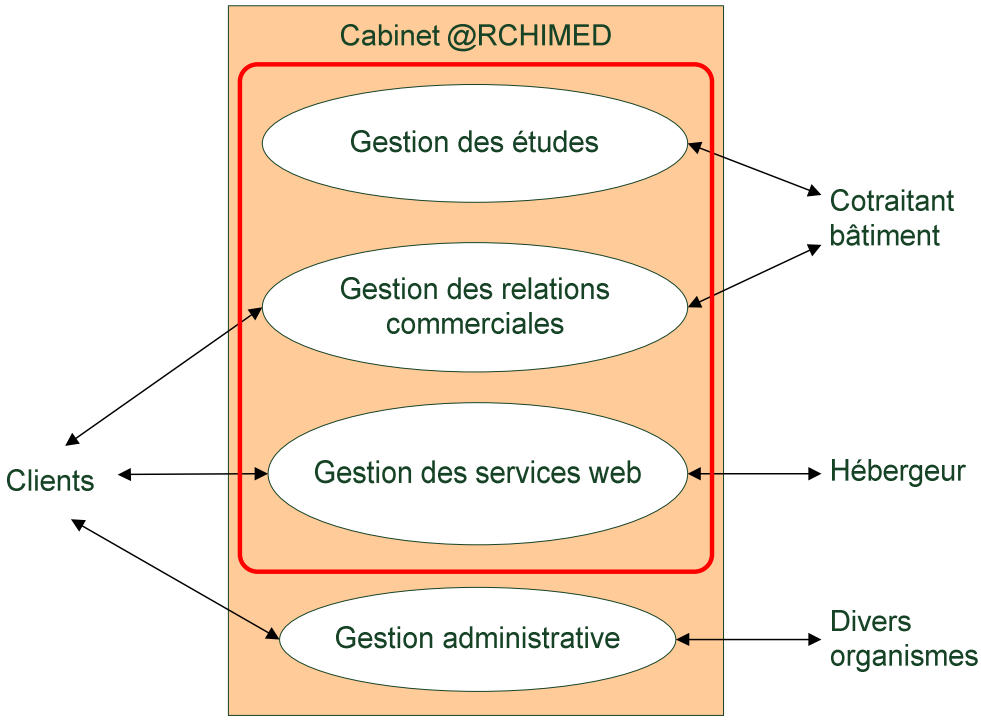

Figure 5 - Le périmètre d'étude

La gestion administrative est donc en dehors du périmètre d'étude :

- gérer la comptabilité ;
- gérer les contentieux juridiques et techniques ;
- gestion administrative interne (ressources humaines, maintenance, assurances) ;
- gestion des permis de construire.

Les principales interfaces concernent :

- les clients (de visu, par téléphone, par courrier papier et électronique),
- les cotraitants bâtiment (de visu, par téléphone, par courrier papier et électronique),
- l'hébergeur du site web (via une connexion Internet, par courrier papier et électronique).

Le système informatique du cabinet @RCHIMED est composé de deux réseaux locaux, l'un pour le bureau d'études et l'autre pour le reste de la société, sur un seul site et dépendant uniquement de la société, utilisés par une douzaine de personnes manipulant des logiciels métiers.

La gestion du site web est assurée par un poste isolé, en relation avec un hébergeur sur Internet.

Le sujet de l'étude représente la partie du système d'information d'@RCHIMED indispensable pour qu'il exerce son métier. L'ensemble du patrimoine informationnel du cabinet est créé, traité et stocké sur ce système d'information.

Les enjeux suivants ont été identifiés :

- favoriser l'ouverture du système informatique vers l'extérieur ;
- démontrer la capacité du cabinet à protéger les projets sensibles (assurer la confidentialité relative aux aspects techniques…) ;
- améliorer les services rendus aux usagers et la qualité des prestations ;
- améliorer les échanges avec les autres organismes (fournisseurs, architectes).

Les participants à l'étude sont définis comme suit :

- la population à l'étude est l'ensemble des collaborateurs travaillant dans le périmètre choisi (gestion des relations commerciales, gestion des études et gestion des services web) ;
- au moins un personnel de chaque catégorie (direction, commercial, ingénieur, technicien) participe à l'étude ; d'autres personnels peuvent également participer à l'étude afin d'apporter un point de vue extérieur ;
- les critères de sélection sont les meilleures connaissances du métier en général, et des processus d'@RCHIMED.

Les paramètres à prendre en compte : des contraintes pour la gestion des risques

Un ensemble de contraintes à prendre en compte a été identifié :

- relatives au personnel :
  - le personnel est utilisateur de l'informatique, mais pas spécialiste,
  - le responsable informatique est l'adjoint du directeur, il est architecte de formation,
  - le personnel de nettoyage intervient de 7h à 8h,
  - la réception des clients se fait dans les bureaux des commerciaux, mais des visites ont parfois lieu au bureau d'études ;
- d'ordre calendaire :
  - la période de pointe se situant d'octobre à mai, toute action (installation de système de sécurité, formation et sensibilisation) se fera en dehors de cette période ;
- d'ordre budgétaire :
  - la société a fait un effort important en matière d'informatisation, tout investissement supplémentaire devra être dûment justifié ;
- d'ordre technique :
  - les règles de conception architecturale doivent être respectées,
  - des logiciels professionnels du domaine architectural doivent être employés ;
- d'environnement :
  - le cabinet loue deux étages d'un immeuble au centre ville,
  - le cabinet est au voisinage de commerces divers,
  - aucun déménagement n'est planifié.

Les sources de menaces

Le cabinet @RCHIMED souhaite s'opposer aux sources de menaces suivantes :

Types de sources de menaces	Retenu ou non	Exemple
Source humaine interne, malveillante, avec de faibles capacités	Non, le cabinet n'estime pas y être exposé	
Source humaine interne, malveillante, avec des capacités importantes	Non, le cabinet n'estime pas y être exposé	
Source humaine interne, malveillante, avec des capacités illimitées	Non, le cabinet n'estime pas y être exposé	
Source humaine externe, malveillante, avec de faibles capacités	Oui	✓ Personnel de nettoyage (soudoyé) ✓ *Script-kiddies*
Source humaine externe, malveillante, avec des capacités importantes	Oui	✓ Concurrent (éventuellement en visite incognito) ✓ Maintenance informatique
Source humaine externe, malveillante, avec des capacités illimitées	Non, le cabinet n'estime pas y être exposé	
Source humaine interne, sans intention de nuire, avec de faibles capacités	Oui	✓ Employé peu sérieux
Source humaine interne, sans intention de nuire, avec des capacités importantes	Non, le cabinet n'estime pas y être exposé	
Source humaine interne, sans intention de nuire, avec des capacités illimitées	Oui	✓ Employé peu sérieux (ceux qui ont un rôle d'administrateur)
Source humaine externe, sans intention de nuire, avec de faibles capacités	Oui	✓ Client ✓ Cotraitant ✓ Partenaire
Source humaine externe, sans intention de nuire, avec des capacités importantes	Oui	✓ Fournisseur d'accès Internet ✓ Hébergeur
Source humaine externe, sans intention de nuire, avec des capacités illimitées	Non, le cabinet n'estime pas y être exposé	
Virus non ciblé	Oui	✓ Virus non ciblé
Phénomène naturel	Oui	✓ Phénomène naturel (foudre, usure…)
Catastrophe naturelle ou sanitaire	Oui	✓ Maladie
Activité animale	Non, le cabinet n'estime pas y être exposé	
Événement interne	Oui	✓ Panne électrique ✓ Incendie des locaux

Les métriques utilisées

Les critères de sécurité retenus : disponibilité, intégrité et confidentialité

Afin d'exprimer les besoins de sécurité, les critères de sécurité retenus sont les suivants :

Critères de sécurité	Définitions
Disponibilité	Propriété d'accessibilité au moment voulu des biens essentiels.
Intégrité	Propriété d'exactitude et de complétude des biens essentiels.
Confidentialité	Propriété des biens essentiels de n'être accessibles qu'aux utilisateurs autorisés.

Échelle de disponibilité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de disponibilité :

Niveaux de l'échelle	Description détaillée de l'échelle
Plus de 72h	Le bien essentiel peut être indisponible plus de 72 heures.
Entre 24 et 72h	Le bien essentiel doit être disponible dans les 72 heures.
Entre 4 et 24h	Le bien essentiel doit être disponible dans les 24 heures.
Moins de 4h	Le bien essentiel doit être disponible dans les 4 heures.

Échelle d'intégrité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes d'intégrité :

Niveaux de l'échelle	Description détaillée de l'échelle
Détectable	Le bien essentiel peut ne pas être intègre si l'altération est identifiée.
Maîtrisé	Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée.
Intègre	Le bien essentiel doit être rigoureusement intègre.

Échelle de confidentialité

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

Niveaux de l'échelle	Description détaillée de l'échelle
Public	Le bien essentiel est public.
Limité	Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires.
Réservé	Le bien essentiel ne doit être accessible qu'au personnel (interne) impliquées.
Privé	Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.

Échelle de gravité

L'échelle suivante sera utilisée pour estimer la gravité des événements redoutés et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
1. Négligeable	@RCHIMED surmontera les impacts sans aucune difficulté.
2. Limitée	@RCHIMED surmontera les impacts malgré quelques difficultés.
3. Importante	@RCHIMED surmontera les impacts avec de sérieuses difficultés.
4. Critique	@RCHIMED ne surmontera pas les impacts (sa survie est menacée).

Échelle de vraisemblance

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
1. Minime	Cela ne devrait pas se (re)produire.
2. Significative	Cela pourrait se (re)produire.
3. Forte	Cela devrait se (re)produire un jour ou l'autre.
4. Maximale	Cela va certainement se (re)produire prochainement.

Les critères de gestion des risques : la liste des règles à utiliser dans l'étude

Les critères de gestion des risques retenus sont les suivants :

Action	Critère de gestion des risques (règle choisie pour réaliser l'action)
Expression des besoins (module 2)	✓ Les besoins de sécurité des biens essentiels sont exprimés à l'aide des échelles correspondantes, selon le critère de sécurité étudié.
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 événements redoutés (module 2)	✓ Les événements redoutés sont classés par ordre décroissant de vraisemblance.
Estimation des scénarios de menaces (module 3)	✓ Les scénarios de menaces sont estimés en termes de vraisemblance 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 considéré. ✓ La vraisemblance d'un risque est égale à la vraisemblance maximale de tous les scénarios de menaces liés à l'événement redouté considéré.
Évaluation des risques (module 4)	✓ Les risques dont la gravité est critique, et ceux dont la gravité est importante et la vraisemblance forte ou maximale, sont jugés comme intolérables. ✓ Les risques dont la gravité est importante et la vraisemblance significative, et ceux dont la gravité est limitée et la vraisemblance forte ou maximale, sont jugés comme significatifs. ✓ Les autres risques sont jugés comme négligeables.
Choix de traitement des risques (module 4)	✓ Les risques intolérables doivent être réduits à un niveau acceptable ou transférés, voire évités si cela est possible. ✓ Les risques significatifs devraient être réduits, transférés ou évités. ✓ Les risques négligeables peuvent être pris.
Homologation de sécurité (module 5)	✓ Le traitement des risques ne peut être validé que s'il est démontré que les risques résiduels sont acceptables et que les mesures de sécurité destinées à traiter les risques peuvent être mises en œuvre dans un délai raisonnable.

Les biens identifiés

Les biens essentiels : 4 processus métiers

Chaque métier sélectionné précédemment dans l'étude est lié à plusieurs processus. Ces processus sont des fonctions qui traitent des informations essentielles en entrée et en sortie.

Dans le cadre du sujet d'étude, le cabinet @RCHIMED a retenu les processus suivants en tant que biens essentiels :

Processus métiers	Processus essentiels	Informations essentielles concernées	Dépositaires
Gestion des relations commerciales	Établir les devis (estimation du coût global d'un projet, négociations avec les clients…)	✓ Cahier des charges ✓ Catalogues techniques ✓ Contrat (demande de réalisation) ✓ Devis	Service commercial
Gestion des études	Créer des plans et calculer les structures	✓ Dossier technique d'un projet ✓ Paramètres techniques (pour les calculs de structure) ✓ Plan technique ✓ Résultat de calcul de structure	Bureau d'études
Gestion des études	Créer des visualisations	✓ Dossier technique d'un projet ✓ Visualisation 3D	Bureau d'études
Gestion des services web	Gérer le contenu du site Internet	✓ Informations société (contacts, présentation…) ✓ Exemple de devis ✓ Exemple de visualisation 3D ✓ Page Web	Directeur adjoint

Les liens entre biens essentiels et biens supports

Le tableau suivant présente les biens supports et leurs liens avec les biens essentiels :

Biens supports \ Biens essentiels	Établir les devis	Créer des plans et calculer les structures	Créer des visualisations	Gérer le contenu du site Internet
Biens supports communs à @RCHIMED				
SYS – Réseau interne	X	X	X	X
MAT – Serveur réseau et fichiers	X	X	X	X
LOG – Serveurs logiciels du réseau interne		X	X	
MAT – Disque USB	X	X	X	
MAT – BOX Wifi	X	X	X	X
MAT – Commutateur	X	X	X	X
MAT – PABX (commutateur téléphonique)	X	X	X	X
MAT – Téléphone fixe	X	X	X	X
MAT – Téléphone portable	X	X	X	X
RSX – Canaux informatiques et de téléphonie	X	X	X	X
ORG – Organisation du cabinet	X	X	X	X
PER – Utilisateur	X	X	X	
PER – Administrateur informatique	X	X	X	X
PAP – Support papier	X	X	X	
CAN – Canaux interpersonnels	X	X	X	X
LOC – Locaux du cabinet	X	X	X	X
Biens supports spécifiques au bureau d'études				
SYS – Sous réseau Ethernet		X	X	
MAT – Ordinateur de design		X	X	
LOG – MacOS X		X	X	
LOG – ARC+ (visualisation)			X	
LOG – Pagemaker (PAO)		X	X	
LOG – Suite bureautique et de messagerie		X	X	
MAT – Ordinateur de calcul et de création		X		
LOG – MacOS X		X		
LOG – SPOT (calculs de résistance)		X		
LOG – Outil de messagerie		X		
LOG – Suite bureautique		X		
RSX – Cordon réseau		X	X	
Biens supports spécifiques aux relations commerciales				
SYS – Sous réseau Wifi	X		X	X
MAT – Ordinateurs portables	X		X	
LOG – Windows XP	X		X	
LOG – Suite bureautique et de messagerie	X		X	
MAT – Ordinateur de mise à jour du site Internet				X
LOG – Windows XP				X
LOG – Logiciel de FTP				X
MAT – Imprimante	X		X	
RSX – Wifi	X		X	X
Partenaires				
SYS – Système de l'hébergeur				X
ORG – Hébergeur				X
SYS – Internet	X			X
ORG – Partenaire	X	X	X	X

Les mesures de sécurité existantes sur les biens supports

@RCHIMED a recensé les mesures de sécurité existantes suivantes :

Mesure de sécurité	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Accord sur le niveau de service de l'hébergeur	ORG – Organisation du cabinet	6.2. Tiers	X		X
Activation d'une alarme anti-intrusion durant les heures de fermeture	LOC – Locaux du cabinet	9.1. Zones sécurisées	X		
Consignes de fermeture à clef des locaux	LOC – Locaux du cabinet	9.1. Zones sécurisées		X	
Dispositifs de lutte contre l'incendie	LOC – Locaux du cabinet	9.1. Zones sécurisées		X	
Climatisation	LOC – Locaux du cabinet	9.2. Sécurité du matériel	X		
Contrat de maintenance informatique (intervention sous 4h)	ORG – Organisation du cabinet	9.2. Sécurité du matériel	X		X
Alimentation secourue	MAT – Serveur réseau et fichiers	9.2. Sécurité du matériel		X	
Installation d'un antivirus sous MacOS X	LOG – MacOS X	10.4. Protection contre les codes malveillant et mobile		X	
Installation d'un antivirus sous Windows XP	LOG – Windows XP	10.4. Protection contre les codes malveillant et mobile		X	
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB	10.5. Sauvegarde			X
Activation du WPA2	MAT – Commutateur	10.6. Gestion de la sécurité des réseaux	X		
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	10.6. Gestion de la sécurité des réseaux	X		
Contrôle d'accès par mot de passe sous MacOS X	LOG – MacOS X	11.5. Contrôle d'accès au système d'exploitation	X		
Contrôle d'accès par mot de passe sous Windows XP	LOG – Windows XP	11.5. Contrôle d'accès au système d'exploitation	X		
Assurance multirisque professionnelle et sur les matériels informatiques	ORG – Organisation du cabinet	14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité			X

Module 2 – Étude des événements redoutés

Les événements redoutés : 12 événements identifiés et estimés

Chaque ligne du tableau suivant représente un événement redouté par le cabinet @RCHIMED (bien essentiel, critère de sécurité, besoin de sécurité selon les échelles de besoin, sources de menaces et impacts). La gravité de chaque évènement redouté est estimée (cf. échelle de gravité) sans tenir compte des mesures de sécurité existantes.

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Établir les devis				
Indisponibilité de devis	24-72h	✓ Employé peu sérieux ✓ Incendie des locaux ✓ Panne électrique	✓ Impossibilité de signer un contrat ✓ Perte d'un marché ✓ Perte de crédibilité	2. Limitée
Altération de devis	Intègre	✓ Employé peu sérieux	✓ Impossibilité de signer un contrat ✓ Perte d'un marché ✓ Impossibilité de remplir les obligations légales ✓ Perte de crédibilité	3. Importante
Compromission de devis	Limité	✓ Employé peu sérieux ✓ Concurrent	✓ Perte d'un marché ✓ Action en justice à l'encontre du cabinet ✓ Perte de crédibilité	3. Importante
Créer des plans et calculer les structures				
Indisponibilité de plans ou de calculs de structures	24-72h	✓ Employé peu sérieux ✓ Virus non ciblé ✓ Personnel de nettoyage (soudoyé) ✓ Personnels de maintenance ✓ Panne électrique	✓ Perte de crédibilité	2. Limitée
Altération de plans ou de calculs de structures	Intègre	✓ Employé peu sérieux ✓ Concurrent	✓ Impossibilité de remplir les obligations légales ✓ Perte de crédibilité ✓ Action en justice à l'encontre du cabinet ✓ Perte de notoriété ✓ Mise en danger (bâtiment qui s'écroule)	4. Critique
Compromission de plans ou calculs de structures	Limité	✓ Employé peu sérieux ✓ Personnel de nettoyage (soudoyé) ✓ Personnels de maintenance	✓ Perte d'un marché ✓ Perte de crédibilité ✓ Perte de notoriété ✓ Impossibilité de remplir les obligations légales (si contractuel)	3. Importante
Créer des visualisations				
Indisponibilité de visualisations	24-72h	✓ Employé peu sérieux ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique	✓ Bouche à oreille négatif ✓ Perte de crédibilité ✓ Perte de notoriété	2. Limitée
Altération de visualisations	Détectable	✓ Employé peu sérieux	✓ Bouche à oreille négatif ✓ Perte de crédibilité ✓ Perte de notoriété	2. Limitée
Compromission de visualisations	Public	-	-	1. Négligeable
Gérer le contenu du site Internet				
Indisponibilité du site Internet	24-72h	✓ Employé peu sérieux ✓ Virus non ciblé ✓ Concurrent ✓ *Script-kiddies* ✓ Panne électrique ✓ Hébergeur	✓ Perte de crédibilité ✓ Perte de notoriété ✓ Bouche à oreille négatif	2. Limitée
Altération du contenu du site Internet	Maîtrisé	✓ Employé peu sérieux ✓ Virus non ciblé ✓ Concurrent ✓ *Script-kiddies* ✓ Hébergeur	✓ Perte de crédibilité ✓ Perte de notoriété ✓ Bouche à oreille négatif ✓ Perte d'un marché ou de clientèle	3. Importante
Compromission du contenu du site Internet	Public	-	-	1. Négligeable

Évaluation : 5 événements redoutés à la gravité critique ou importante

L'importance relative des événements redoutés précédemment analysés (identifiés et estimés) est évaluée à l'aide du tableau suivant (cf. critères de gestion des risques) :

Gravité	Événements redoutés
4. Critique	✓ Altération de plans ou de calculs de structures
3. Importante	✓ Altération de devis ✓ Compromission de plans ou calculs de structures ✓ Compromission de devis ✓ Altération du contenu du site Internet
2. Limitée	✓ Indisponibilité de devis ✓ Indisponibilité de visualisations ✓ Altération de visualisations ✓ Indisponibilité de plans ou de calculs de structures ✓ Indisponibilité du site Internet
1. Négligeable	✓ Compromission de visualisations ✓ Compromission du contenu du site Internet

Module 3 – Étude des scénarios de menaces

Les scénarios de menaces : 24 scénarios identifiés et estimés

Les pages suivantes présentent les scénarios de menaces potentiellement réalisables dans le cadre du sujet de l'étude.

Les sources de menaces susceptibles d'en être à l'origine sont identifiées et la vraisemblance de chaque scénario de menace est estimée (cf. échelle de vraisemblance).

Le détail des scénarios de menaces (menaces, vulnérabilités et pré-requis) est décrit dans les bases de connaissances de la méthode EBIOS.

Scénarios de menaces	Sources de menaces	Vraisemblance
SYS – Réseau interne		
Menaces sur le réseau interne causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le réseau interne causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	2. Significative
Menaces sur le réseau interne causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	2. Significative
SYS – Sous réseau Ethernet		
Menaces sur le sous réseau Ethernet causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le sous réseau Ethernet causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	2. Significative
Menaces sur le sous réseau Ethernet causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	2. Significative
SYS – Sous réseau Wifi		
Menaces sur le sous réseau Wifi causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le sous réseau Wifi causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	3. Forte
Menaces sur le sous réseau Wifi causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	3. Forte
ORG – Organisation du cabinet		
Menaces sur l'organisation d'@RCHIMED causant une indisponibilité	✓ Employé peu sérieux ✓ Personnel de nettoyage ✓ Maladie	2. Significative
Menaces sur l'organisation d'@RCHIMED causant une altération	✓ Employé peu sérieux ✓ Personnel de nettoyage	1. Minime
Menaces sur l'organisation d'@RCHIMED causant une compromission	✓ Concurrent (en visite incognito) ✓ Employé peu sérieux ✓ Cotraitant ✓ Client ✓ Maintenance informatique ✓ Personnel de nettoyage	4. Maximale
SYS – Système de l'hébergeur		

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le système de l'hébergeur causant une indisponibilité	✓ Hébergeur ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	4. Maximale
Menaces sur le système de l'hébergeur causant une altération	✓ Hébergeur ✓ *Script-kiddies* ✓ Virus non ciblé	3. Forte
Menaces sur le système de l'hébergeur causant une compromission	✓ Concurrent ✓ Client ✓ Partenaire	4. Maximale
ORG – Hébergeur		
Menaces sur l'hébergeur causant une indisponibilité	✓ Hébergeur	2. Significative
Menaces sur l'hébergeur causant une altération	✓ Hébergeur	2. Significative
Menaces sur l'hébergeur causant une compromission	✓ Hébergeur	1. Minime
SYS – Internet		
Menaces sur Internet causant une indisponibilité	✓ Fournisseur d'accès Internet	2. Significative
Menaces sur Internet causant une altération	✓ *Script-kiddies*	1. Minime
Menaces sur Internet causant une compromission	✓ *Script-kiddies* ✓ Concurrent	2. Significative
ORG – Partenaire		
Menaces sur un partenaire causant une indisponibilité	✓ Partenaire	3. Forte
Menaces sur un partenaire causant une altération	✓ Partenaire	1. Minime
Menaces sur un partenaire causant une compromission	✓ Partenaire	4. Maximale

Évaluation : 11 scénarios de menaces à la vraisemblance maximale ou forte

L'importance relative des scénarios de menaces précédemment analysés (identifiés et estimés) est évaluée de la façon suivante (cf. critères de gestion des risques) :

Vraisemblance	Scénarios de menaces
4. Maximale	✓ Menaces sur l'organisation d'@RCHIMED causant une compromission ✓ Menaces sur le système de l'hébergeur causant une indisponibilité ✓ Menaces sur le système de l'hébergeur causant une compromission ✓ Menaces sur un partenaire causant une compromission
3. Forte	✓ Menaces sur le réseau interne causant une indisponibilité ✓ Menaces sur le sous réseau Ethernet causant une indisponibilité ✓ Menaces sur le sous réseau Wifi causant une indisponibilité ✓ Menaces sur le sous réseau Wifi causant une altération ✓ Menaces sur le sous réseau Wifi causant une compromission ✓ Menaces sur le système de l'hébergeur causant une altération ✓ Menaces sur un partenaire causant une indisponibilité
2. Significative	✓ Menaces sur le réseau interne causant une altération ✓ Menaces sur le réseau interne causant une compromission ✓ Menaces sur le sous réseau Ethernet causant une altération ✓ Menaces sur le sous réseau Ethernet causant une compromission ✓ Menaces sur l'organisation d'@RCHIMED causant une indisponibilité ✓ Menaces sur l'hébergeur causant une indisponibilité ✓ Menaces sur l'hébergeur causant une altération ✓ Menaces sur Internet causant une indisponibilité ✓ Menaces sur Internet causant une compromission
1. Minime	✓ Menaces sur l'organisation d'@RCHIMED causant une altération ✓ Menaces sur l'hébergeur causant une compromission ✓ Menaces sur Internet causant une altération ✓ Menaces sur un partenaire causant une altération

Module 4 – Étude des risques

Les risques : 12 risques analysés

@RCHIMED a établi la liste des risques à partir des événements redoutés et des scénarios de menaces précédemment appréciés.
Les mesures de sécurité existantes ayant un effet sur chaque risque ont également été identifiées.
La gravité et la vraisemblance ont finalement été estimées, sans, puis avec, les mesures de sécurité (les niveaux rayés correspondent aux valeurs avant application de ces mesures).

Risque lié à l'indisponibilité d'un devis au-delà de 72h

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Indisponibilité de devis	24-72h	✓ Employé peu sérieux ✓ Incendie des locaux ✓ Panne électrique	✓ Impossibilité de signer un contrat ✓ Perte d'un marché ✓ Perte de crédibilité	2. Limitée

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le sous réseau Wifi causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une indisponibilité	✓ Employé peu sérieux ✓ Personnel de nettoyage ✓ Maladie	2. Significative
Menaces sur Internet causant une indisponibilité	✓ Fournisseur d'accès Internet	2. Significative
Menaces sur un partenaire causant une indisponibilité	✓ Partenaire	3. Forte

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation du WPA2	MAT – Commutateur	X		
Assurance multirisque professionnelle et sur les matériels informatiques	ORG – Organisation du cabinet			X
Climatisation	LOC – Locaux du cabinet	X		
Contrat de maintenance informatique (intervention sous 4h)	ORG – Organisation du cabinet	X		X
Contrôle d'accès par mot de passe	LOG – Windows XP	X		
Dispositifs de lutte contre l'incendie	LOC – Locaux du cabinet		X	
Installation d'un antivirus	LOG – Windows XP		X	
Alimentation secourue	MAT – Serveur réseau et fichiers		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Altération de devis	Intègre	✓ Employé peu sérieux	✓ Impossibilité de signer un contrat ✓ Perte d'un marché ✓ Impossibilité de remplir les obligations légales ✓ Perte de crédibilité	3. Importante

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	2. Significative
Menaces sur le sous réseau Wifi causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une altération	✓ Employé peu sérieux ✓ Personnel de nettoyage	1. Minime
Menaces sur Internet causant une altération	✓ *Script-kiddies*	1. Minime
Menaces sur un partenaire causant une altération	✓ Partenaire	1. Minime

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation du WPA2	MAT – Commutateur	X		
Contrat de maintenance informatique (intervention sous 4h)	ORG – Organisation du cabinet	X		X
Contrôle d'accès par mot de passe	LOG – Windows XP	X		
Installation d'un antivirus	LOG – Windows XP		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Risque lié à la compromission d'un devis au-delà du personnel et des partenaires

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Compromission de devis	Limité	✓ Employé peu sérieux ✓ Concurrent	✓ Perte d'un marché ✓ Action en justice à l'encontre du cabinet ✓ Perte de crédibilité	3. Importante

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	2. Significative
Menaces sur le sous réseau Wifi causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une compromission	✓ Concurrent (en visite incognito) ✓ Employé peu sérieux ✓ Cotraitant ✓ Client ✓ Maintenance informatique ✓ Personnel de nettoyage	4. Maximale
Menaces sur Internet causant une compromission	✓ *Script-kiddies* ✓ Concurrent	2. Significative
Menaces sur un partenaire causant une compromission	✓ Partenaire	4. Maximale

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation d'une alarme anti-intrusion durant les heures de fermeture	LOC – Locaux du cabinet	X		
Activation du WPA2	MAT – Commutateur	X		
Assurance multirisque professionnelle et sur les matériels informatiques	ORG – Organisation du cabinet			X
Consignes de fermeture à clef des locaux	LOC – Locaux du cabinet		X	
Contrôle d'accès par mot de passe	LOG – Windows XP	X		
Installation d'un antivirus	LOG – Windows XP		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		

Niveau de risque				
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	3. Forte	**4. Maximale**

Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Indisponibilité de plans ou de calculs de structures	24-72h	✓ Employé peu sérieux ✓ Virus non ciblé ✓ Personnel de nettoyage (soudoyé) ✓ Personnels de maintenance ✓ Panne électrique	✓ Perte de crédibilité	2. Limitée

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le sous réseau Ethernet causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une indisponibilité	✓ Employé peu sérieux ✓ Personnel de nettoyage ✓ Maladie	2. Significative
Menaces sur un partenaire causant une indisponibilité	✓ Partenaire	3. Forte

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation du WPA2	MAT – Commutateur	X		
Assurance multirisque professionnelle et sur les matériels informatiques	ORG – Organisation du cabinet			X
Climatisation	LOC – Locaux du cabinet	X		
Contrat de maintenance informatique (intervention sous 4h)	ORG – Organisation du cabinet	X		X
Contrôle d'accès par mot de passe	LOG – MacOS X	X		
Dispositifs de lutte contre l'incendie	LOC – Locaux du cabinet		X	
Installation d'un antivirus	LOG – MacOS X		X	
Alimentation secourue	MAT – Serveur réseau et fichiers		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Altération de plans ou de calculs de structures	Intègre	✓ Employé peu sérieux ✓ Concurrent	✓ Impossibilité de remplir les obligations légales ✓ Perte de crédibilité ✓ Action en justice à l'encontre du cabinet ✓ Perte de notoriété ✓ Mise en danger (bâtiment qui s'écroule)	4. Critique

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	2. Significative
Menaces sur le sous réseau Ethernet causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	2. Significative
Menaces sur l'organisation d'@RCHIMED causant une altération	✓ Employé peu sérieux ✓ Personnel de nettoyage	1. Minime
Menaces sur un partenaire causant une altération	✓ Partenaire	1. Minime

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation du WPA2	MAT – Commutateur	X		
Contrat de maintenance informatique (intervention sous 4h)	ORG – Organisation du cabinet	X		X
Contrôle d'accès par mot de passe	LOG – MacOS X	X		
Installation d'un antivirus	LOG – MacOS X		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	1. Négligeable	2. Limitée	3. Importante	**4. Critique**
Vraisemblance	1. Minime	**2. Significative**	3. Forte	4. Maximale

Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Compromission de plans ou calculs de structures	Limité	✓ Employé peu sérieux ✓ Personnel de nettoyage (soudoyé) ✓ Personnels de maintenance	✓ Perte d'un marché ✓ Perte de crédibilité ✓ Perte de notoriété ✓ Impossibilité de remplir les obligations légales (si contractuel)	3. Importante

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	2. Significative
Menaces sur le sous réseau Ethernet causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	2. Significative
Menaces sur l'organisation d'@RCHIMED causant une compromission	✓ Concurrent (en visite incognito) ✓ Employé peu sérieux ✓ Cotraitant ✓ Client ✓ Maintenance informatique ✓ Personnel de nettoyage	4. Maximale
Menaces sur un partenaire causant une compromission	✓ Partenaire	4. Maximale

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation d'une alarme anti-intrusion durant les heures de fermeture	LOC – Locaux du cabinet	X		
Activation du WPA2	MAT – Commutateur	X		
Consignes de fermeture à clef des locaux	LOC – Locaux du cabinet		X	
Contrôle d'accès par mot de passe	LOG – MacOS X	X		
Installation d'un antivirus	LOG – MacOS X		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		

Niveau de risque				
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	2. Significative	3. Forte	**4. Maximale**

Risque lié à l'indisponibilité de visualisations au-delà de 72h

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Indisponibilité de visualisations	24-72h	✓ Employé peu sérieux ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique	✓ Bouche à oreille négatif ✓ Perte de crédibilité ✓ Perte de notoriété	2. Limitée

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le sous réseau Ethernet causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le sous réseau Wifi causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une indisponibilité	✓ Employé peu sérieux ✓ Personnel de nettoyage ✓ Maladie	2. Significative
Menaces sur un partenaire causant une indisponibilité	✓ Partenaire	3. Forte

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation du WPA2	MAT – Commutateur	X		
Assurance multirisque professionnelle et sur les matériels informatiques	ORG – Organisation du cabinet			X
Climatisation	LOC – Locaux du cabinet	X		
Contrat de maintenance informatique (intervention sous 4h)	ORG – Organisation du cabinet	X		X
Contrôle d'accès par mot de passe	LOG – MacOS X	X		
Contrôle d'accès par mot de passe	LOG – Windows XP	X		
Dispositifs de lutte contre l'incendie	LOC – Locaux du cabinet		X	
Installation d'un antivirus	LOG – MacOS X		X	
Installation d'un antivirus	LOG – Windows XP		X	
Alimentation secourue	MAT – Serveur réseau et fichiers		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Risque lié à l'altération de visualisations sans pouvoir la détecter

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Altération de visualisations	Détectable	✓ Employé peu sérieux	✓ Bouche à oreille négatif ✓ Perte de crédibilité ✓ Perte de notoriété	2. Limitée

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	2. Significative
Menaces sur le sous réseau Ethernet causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	2. Significative
Menaces sur le sous réseau Wifi causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une altération	✓ Employé peu sérieux ✓ Personnel de nettoyage	1. Minime
Menaces sur un partenaire causant une altération	✓ Partenaire	1. Minime

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation du WPA2	MAT – Commutateur	X		
Contrat de maintenance informatique (intervention sous 4h)	ORG – Organisation du cabinet	X		X
Contrôle d'accès par mot de passe	LOG – MacOS X	X		
Contrôle d'accès par mot de passe	LOG – Windows XP	X		
Installation d'un antivirus	LOG – MacOS X		X	
Installation d'un antivirus	LOG – Windows XP		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	**3. Forte**	4. Maximale

Risque lié à la compromission de visualisations, jugées comme publiques

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Compromission de visualisations	Public	-	-	1. Négligeable

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	2. Significative
Menaces sur le sous réseau Ethernet causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	2. Significative
Menaces sur le sous réseau Wifi causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une compromission	✓ Concurrent (en visite incognito) ✓ Employé peu sérieux ✓ Cotraitant ✓ Client ✓ Maintenance informatique ✓ Personnel de nettoyage	4. Maximale
Menaces sur un partenaire causant une compromission	✓ Partenaire	4. Maximale

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation d'une alarme anti-intrusion durant les heures de fermeture	LOC – Locaux du cabinet	X		
Activation du WPA2	MAT – Commutateur	X		
Consignes de fermeture à clef des locaux	LOC – Locaux du cabinet		X	
Contrôle d'accès par mot de passe	LOG – MacOS X	X		
Contrôle d'accès par mot de passe	LOG – Windows XP	X		
Installation d'un antivirus	LOG – MacOS X		X	
Installation d'un antivirus	LOG – Windows XP		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	**1. Négligeable**	2. Limitée	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	3. Forte	**4. Maximale**

Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Indisponibilité du site Internet	24-72h	✓ Employé peu sérieux ✓ Virus non ciblé ✓ Concurrent ✓ *Script-kiddies* ✓ Panne électrique ✓ Hébergeur	✓ Perte de crédibilité ✓ Perte de notoriété ✓ Bouche à oreille négatif	2. Limitée

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le sous réseau Ethernet causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur le sous réseau Wifi causant une indisponibilité	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Incendie des locaux ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une indisponibilité	✓ Employé peu sérieux ✓ Personnel de nettoyage ✓ Maladie	2. Significative
Menaces sur le système de l'hébergeur causant une indisponibilité	✓ Hébergeur ✓ *Script-kiddies* ✓ Virus non ciblé ✓ Panne électrique ✓ Phénomène naturel (foudre, usure…)	4. Maximale
Menaces sur l'hébergeur causant une indisponibilité	✓ Hébergeur	2. Significative
Menaces sur Internet causant une indisponibilité	✓ Fournisseur d'accès Internet	2. Significative
Menaces sur un partenaire causant une indisponibilité	✓ Partenaire	3. Forte

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Accord sur le niveau de service de l'hébergeur	ORG – Organisation du cabinet	X		X
Activation du WPA2	MAT – Commutateur	X		
Assurance multirisque professionnelle et sur les matériels informatiques	ORG – Organisation du cabinet			X
Climatisation	LOC – Locaux du cabinet	X		
Contrat de maintenance informatique (intervention sous 4h)	ORG – Organisation du cabinet	X		X
Contrôle d'accès par mot de passe	LOG – Windows XP	X		
Dispositifs de lutte contre l'incendie	LOC – Locaux du cabinet		X	
Installation d'un antivirus	LOG – Windows XP		X	
Alimentation secourue	MAT – Serveur réseau et fichiers		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	~~4. Maximale~~

Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Altération du contenu du site Internet	Maîtrisé	✓ Employé peu sérieux ✓ Virus non ciblé ✓ Concurrent ✓ *Script-kiddies* ✓ Hébergeur	✓ Perte de crédibilité ✓ Perte de notoriété ✓ Bouche à oreille négatif ✓ Perte d'un marché ou de clientèle	3. Importante

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	2. Significative
Menaces sur le sous réseau Ethernet causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	2. Significative
Menaces sur le sous réseau Wifi causant une altération	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies* ✓ Virus non ciblé	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une altération	✓ Employé peu sérieux ✓ Personnel de nettoyage	1. Minime
Menaces sur le système de l'hébergeur causant une altération	✓ Hébergeur ✓ *Script-kiddies* ✓ Virus non ciblé	3. Forte
Menaces sur l'hébergeur causant une altération	✓ Hébergeur	2. Significative
Menaces sur Internet causant une altération	✓ *Script-kiddies*	1. Minime
Menaces sur un partenaire causant une altération	✓ Partenaire	1. Minime

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Accord sur le niveau de service de l'hébergeur	ORG – Organisation du cabinet	X		X
Activation du WPA2	MAT – Commutateur	X		
Contrat de maintenance informatique (intervention sous 4h)	ORG – Organisation du cabinet	X		X
Contrôle d'accès par mot de passe	LOG – Windows XP	X		
Installation d'un antivirus	LOG – Windows XP		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

Risque lié à la compromission du contenu du site Internet public

Événement redouté	Besoin de sécurité	Sources de menaces	Impacts	Gravité
Compromission du contenu du site Internet	Public	-	-	1. Négligeable

Scénarios de menaces	Sources de menaces	Vraisemblance
Menaces sur le réseau interne causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	2. Significative
Menaces sur le sous réseau Ethernet causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	2. Significative
Menaces sur le sous réseau Wifi causant une compromission	✓ Employé peu sérieux ✓ Maintenance informatique ✓ *Script-kiddies*	3. Forte
Menaces sur l'organisation d'@RCHIMED causant une compromission	✓ Concurrent (en visite incognito) ✓ Employé peu sérieux ✓ Cotraitant ✓ Client ✓ Maintenance informatique ✓ Personnel de nettoyage	4. Maximale
Menaces sur le système de l'hébergeur causant une compromission	✓ Concurrent ✓ Client ✓ Partenaire	4. Maximale
Menaces sur l'hébergeur causant une compromission	✓ Hébergeur	1. Minime
Menaces sur Internet causant une compromission	✓ *Script-kiddies* ✓ Concurrent	2. Significative
Menaces sur un partenaire causant une compromission	✓ Partenaire	4. Maximale

Mesure de sécurité existante	Bien support sur lequel elle repose	Prévention	Protection	Récupération
Activation d'une alarme anti-intrusion durant les heures de fermeture	LOC – Locaux du cabinet	X		
Activation du WPA2	MAT – Commutateur	X		
Consignes de fermeture à clef des locaux	LOC – Locaux du cabinet		X	
Contrôle d'accès par mot de passe	LOG – MacOS X	X		
Contrôle d'accès par mot de passe	LOG – Windows XP	X		
Installation d'un antivirus	LOG – MacOS X		X	
Installation d'un antivirus	LOG – Windows XP		X	
Accès restreint en entrée (messagerie, services WEB…)	MAT – Commutateur	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans une armoire fermant à clef	MAT – Disque USB			X

Niveau de risque				
Gravité	**1. Négligeable**	2. Limitée	3. Importante	4. Critique
Vraisemblance	1. Minime	2. Significative	3. Forte	**4. Maximale**

Évaluation : 4 risques intolérables et 2 risques significatifs

Les risques précédemment analysés (identifiés et estimés) peuvent être évalués à l'aide du tableau suivant (les risques rayés correspondent à ceux réduits par des mesures de sécurité existantes) :

Gravité					
	4. Critique		✓ Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres		
	3. Importante		✓ Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	✓ Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre ✓ ~~Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver~~	✓ Risque lié à la compromission d'un devis au-delà du personnel et des partenaires ✓ Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires
	2. Limitée		✓ Risque lié à l'indisponibilité d'un devis au-delà de 72h ✓ Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h ✓ Risque lié à l'indisponibilité de visualisations au-delà de 72h ✓ Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h	✓ ~~Risque lié à l'indisponibilité d'un devis au-delà de 72h~~ ✓ ~~Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h~~ ✓ ~~Risque lié à l'indisponibilité de visualisations au-delà de 72h~~ ✓ Risque lié à l'altération de visualisations sans pouvoir la détecter	✓ ~~Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h~~
	1. Négligeable				✓ Risque lié à la compromission de visualisations, jugées comme publiques ✓ Risque lié à la compromission du contenu du site Internet public
		1. Minime	**2. Significative**	**3. Forte**	**4. Maximale**
		Vraisemblance			

Légende :

Risques négligeables	Risques significatifs	Risques intolérables

Les objectifs de sécurité : 6 risques à réduire et/ou à transférer en priorité

@RCHIMED souhaite essentiellement réduire les risques jugés comme prioritaires et significatifs, et prendre les risques jugés comme non prioritaires.

Le tableau suivant présente les objectifs de sécurité identifiés (les croix correspondent aux premiers choix, les croix entre parenthèses correspondent aux autres possibilités acceptées) :

Risque	Évitement	Réduction	Prise	Transfert
Risque lié à l'indisponibilité d'un devis au-delà de 72h		(X)	X	
Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	(X)	X	X	(X)
Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	(X)	X	X	(X)
Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h		(X)	X	
Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	(X)	X	X	(X)
Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	(X)	X	X	(X)
Risque lié à l'indisponibilité de visualisations au-delà de 72h		(X)	X	
Risque lié à l'altération de visualisations sans pouvoir la détecter		X	(X)	(X)
Risque lié à la compromission de visualisations, jugées comme publiques		(X)	X	
Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h		(X)	X	
Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver		X	(X)	(X)
Risque lié à la compromission du contenu du site Internet public		(X)	X	

Les risques résiduels : 6 risques jugés comme négligeables

À l'issue de l'identification des objectifs de sécurité, @RCHIMED a mis en évidence les risques résiduels suivants :

Risques résiduels	Gravité	Vraisemblance
Risque lié à l'indisponibilité d'un devis au-delà de 72h	2. Limitée	2. Significative
Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h	2. Limitée	2. Significative
Risque lié à l'indisponibilité de visualisations au-delà de 72h	2. Limitée	2. Significative
Risque lié à la compromission de visualisations, jugées comme publiques	1. Négligeable	4. Maximale
Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h	2. Limitée	2. Significative
Risque lié à la compromission du contenu du site Internet public	1. Négligeable	4. Maximale

On note que ces risques résiduels pourront être réduits ultérieurement, quand les autres risques seront devenus acceptables.

Module 5 – Étude des mesures de sécurité

Les mesures de sécurité : une défense en profondeur pour réduire et transférer les risques

Le tableau suivant présente la liste des mesures de sécurité destinées à réduire ou transférer les risques prioritaires (elles traitent également les autres risques) :

Mesure de sécurité	Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	Risque lié à l'altération de visualisations sans pouvoir la détecter	Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Interdiction d'accès aux locaux à toute personne (dont le personnel de nettoyage) sans la présence de membres du personnel	X	X	X	X	X	X	LOC – Locaux du cabinet	9.1. Zones sécurisées	X		
Pose de barreaux aux fenêtres		X		X			LOC – Locaux du cabinet	9.1. Zones sécurisées	X		
Dispositifs de lutte contre l'incendie	X	X	X	X	X	X	LOC – Locaux du cabinet	9.1. Zones sécurisées		X	
Activation d'une alarme anti-intrusion durant les heures de fermeture		X		X			LOC – Locaux du cabinet	9.1. Zones sécurisées	X		
Consignes de fermeture à clef des locaux		X		X			LOC – Locaux du cabinet	9.1. Zones sécurisées		X	
Climatisation							LOC – Locaux du cabinet	9.2. Sécurité du matériel	X		
Chiffrement des fichiers liés aux plans et calculs de structures à l'aide de certificats électroniques				X			LOG – MacOS X	7.1. Responsabilités relatives aux biens		X	
Désactivation des composants inutiles sur MacOS X				X			LOG – MacOS X	10.1. Procédures et responsabilités liées à l'exploitation	X		
Installation d'un antivirus sous MacOS X			X		X		LOG – MacOS X	10.4. Protection contre les codes malveillant et mobile		X	
Contrôle d'accès par mot de passe sous MacOS X				X			LOG – MacOS X	11.5. Contrôle d'accès au système d'exploitation	X		

Mesure de sécurité	Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	Risque lié à l'altération de visualisations sans pouvoir la détecter	Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Désactivation des composants inutiles sur le serveur	X	X	X	X	X	X	LOG – Serveurs logiciels du réseau interne	10.1. Procédures et responsabilités liées à l'exploitation	X		
Installation d'un antivirus sur les serveurs	X		X		X	X	LOG – Serveurs logiciels du réseau interne	10.4. Protection contre les codes malveillant et mobile		X	
Test trimestriel des fichiers sauvegardés	X		X		X	X	LOG – Serveurs logiciels du réseau interne	10.5. Sauvegarde			X
Vérification des empreintes des fichiers liés aux devis de manière régulière	X		X		X	X	LOG – Serveurs logiciels du réseau interne	10.10. Surveillance		X	
Journalisation des événements informatiques (accès, erreurs…)	X	X	X	X	X	X	LOG – Serveurs logiciels du réseau interne	10.10. Surveillance		X	X
Accès uniquement aux services nécessaires	X	X	X	X	X	X	LOG – Serveurs logiciels du réseau interne	11.4. Contrôle d'accès au réseau	X		
Restriction des accès nécessaires pour la maintenance		X		X			LOG – Serveurs logiciels du réseau interne	11.6. Contrôle d'accès aux applications et à l'information	X		
Mise en place d'un système RAID logiciel	X		X		X		LOG – Serveurs logiciels du réseau interne	12.2. Bon fonctionnement des applications		X	X
Gestion des vulnérabilités sur les serveurs	X	X	X	X	X	X	LOG – Serveurs logiciels du réseau interne	12.6. Gestion des vulnérabilités techniques	X		
Gestion des vulnérabilités sur Windows XP	X	X	X	X	X	X	LOG – Serveurs logiciels du réseau interne	12.6. Gestion des vulnérabilités techniques	X		

Mesure de sécurité	Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	Risque lié à l'altération de visualisations sans pouvoir la détecter	Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Gestion des vulnérabilités sur MacOS X			X	X	X		LOG – Serveurs logiciels du réseau interne	12.6. Gestion des vulnérabilités techniques	X		
Utilisation du mode "corrections apparentes" lors des échanges lors de l'établissement des devis	X						LOG – Suite bureautique et de messagerie	7.1. Responsabilités relatives aux biens		X	
Chiffrement des fichiers liés aux devis à l'aide de certificats électroniques		X					LOG – Windows XP	7.1. Responsabilités relatives aux biens		X	
Désactivation des composants inutiles sur Windows XP	X	X	X		X	X	LOG – Windows XP	10.1. Procédures et responsabilités liées à l'exploitation	X		
Installation d'un antivirus sous Windows XP	X		X		X	X	LOG – Windows XP	10.4. Protection contre les codes malveillant et mobile		X	
Mise à jour régulière de l'antivirus des serveurs et de sa base de signatures	X		X		X	X	LOG – Windows XP	10.4. Protection contre les codes malveillant et mobile		X	
Mise à jour régulière de l'antivirus sous Windows XP et de sa base de signatures	X		X		X	X	LOG – Windows XP	10.4. Protection contre les codes malveillant et mobile		X	
Mise à jour régulière de l'antivirus sous MacOS X et de sa base de signatures			X		X		LOG – Windows XP	10.4. Protection contre les codes malveillant et mobile		X	
Sauvegarde du site Internet à chaque mise à jour						X	LOG – Windows XP	10.5. Sauvegarde			X
Sauvegarde immédiate des fichiers liés aux devis sur des disques USB stockés dans un meuble fermant à clef	X		X		X		LOG – Windows XP	10.5. Sauvegarde			X
Mise en place d'un système de vérification d'intégrité du site Internet						X	LOG – Windows XP	10.9. Services de commerce électronique		X	
Contrôle d'accès par mot	X	X	X		X	X	LOG –	11.5. Contrôle d'accès	X		

Mesure de sécurité	Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	Risque lié à l'altération de visualisations sans pouvoir la détecter	Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
de passe sous Windows XP							Windows XP	au système d'exploitation			
Création d'empreintes des fichiers liés aux devis	X		X		X	X	LOG – Windows XP	11.3. Responsabilités utilisateurs		X	
Création d'empreintes des fichiers liés aux plans et aux calculs de structure			X				LOG – Windows XP	11.3. Responsabilités utilisateurs		X	
Création d'empreintes des fichiers liés aux visualisations					X		LOG – Windows XP	11.3. Responsabilités utilisateurs		X	
Création d'empreintes des fichiers sauvegardés du site Internet						X	LOG – Windows XP	11.3. Responsabilités utilisateurs		X	
Accès restreint en entrée (messagerie, services WEB…)	X	X	X	X	X	X	MAT – Commutateur	10.6. Gestion de la sécurité des réseaux	X		
Activation du WPA2	X	X	X	X	X	X	MAT – Commutateur	10.6. Gestion de la sécurité des réseaux	X		
Sauvegarde hebdomadaire sur des disques USB stockés dans un meuble fermant à clef	X		X		X	X	MAT – Disque USB	10.5. Sauvegarde			X
Rangement des supports amovibles dans un meuble fermant à clef		X		X			MAT – Disque USB	10.7. Manipulation des supports	X		
Utilisation d'antivols pour les ordinateurs portables		X		X			MAT – Ordinateurs portables	9.2. Sécurité du matériel	X		X
Utilisation de films empêchant l'espionnage de l'écran des ordinateurs portables		X		X			MAT – Ordinateurs portables	9.2. Sécurité du matériel	X		X
Limitation des informations sensibles sur les ordinateurs portables		X		X			MAT – Ordinateurs portables	11.7. Informatique mobile et télétravail	X		
Alimentation secourue							MAT – Serveur réseau et fichiers	9.2. Sécurité du matériel		X	

Mesure de sécurité	Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	Risque lié à l'altération de visualisations sans pouvoir la détecter	Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Élaboration d'une politique de sécurité de l'information	X	X	X	X	X	X	ORG – Organisation du cabinet	5.1. Politique de sécurité de l'information	X	X	X
Révision de la politique de sécurité de l'information au moins une fois par an	X	X	X	X	X	X	ORG – Organisation du cabinet	5.1. Politique de sécurité de l'information	X	X	X
Soutien de la direction vis-à-vis de la sécurité de l'information	X	X	X	X	X	X	ORG – Organisation du cabinet	6.1. Organisation interne	X	X	X
Définition des responsabilités en matière de sécurité de l'information	X	X	X	X	X	X	ORG – Organisation du cabinet	6.1. Organisation interne	X	X	X
Identification des exigences en matière d'engagement de confidentialité		X		X			ORG – Organisation du cabinet	6.1. Organisation interne	X	X	X
Accompagnement systématique des visiteurs dans les locaux		X		X			ORG – Organisation du cabinet	6.2. Tiers	X	X	
Enregistrement systématique des visiteurs		X		X			ORG – Organisation du cabinet	6.2. Tiers	X		
Signature d'un engagement de confidentialité par les cotraitants, les clients, la maintenance, le personnel de nettoyage et les partenaires		X		X			ORG – Organisation du cabinet	6.2. Tiers	X		X
Inventaire des biens sensibles	X	X	X	X	X	X	ORG – Organisation du cabinet	7.1. Responsabilités relatives aux biens	X	X	X
Adoption d'une politique de nommage des fichiers et des versions successives	X		X		X		ORG – Organisation du cabinet	7.1. Responsabilités relatives aux biens	X		
Marquage du besoin de confidentialité des documents électroniques liés aux devis		X		X			ORG – Organisation du cabinet	7.2. Classification des informations	X		

Mesure de sécurité	Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	Risque lié à l'altération de visualisations sans pouvoir la détecter	Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Signature d'un engagement de confidentialité par les personnels		X		X			ORG – Organisation du cabinet	8.1. Avant le recrutement	X		X
Utilisation de scellés sur les ordinateurs afin de pouvoir constater leur ouverture non désirée	X	X	X	X	X	X	ORG – Organisation du cabinet	9.2. Sécurité du matériel	X		X
Contrat de maintenance informatique (intervention sous 4h)	X		X		X	X	ORG – Organisation du cabinet	9.2. Sécurité du matériel	X		X
Accord sur le niveau de service de l'hébergeur						X	ORG – Organisation du cabinet	10.2. Gestion de la prestation de service par un tiers	X		X
Établissement d'un accord d'échange d'informations avec les clients et les partenaires		X		X			ORG – Organisation du cabinet	10.8. Échange des informations	X		
Contrôle annuel de l'application des mesures de sécurité	X	X	X	X	X	X	ORG – Organisation du cabinet	15.3. Prises en compte de l'audit du système d'information	X		
Détermination des droits d'accès selon le métier	X	X	X	X	X	X	ORG – Organisation du cabinet	11.1. Exigences métier relatives au contrôle d'accès	X		
Adoption d'une politique de moindre privilège	X	X	X	X	X	X	ORG – Organisation du cabinet	11.2. Gestion de l'accès utilisateur	X		
Utilisation d'un identifiant unique	X	X	X	X	X	X	ORG – Organisation du cabinet	11.5. Contrôle d'accès au système d'exploitation	X		
Formalisation d'une politique de gestion des mesures cryptographiques (chiffrement, création d'empreintes…)	X	X	X	X	X		ORG – Organisation du cabinet	12.3. Mesures cryptographiques	X		
Conservation de preuves conformément aux dispositions légales		X		X			ORG – Organisation du cabinet	13.2. Gestion des améliorations et incidents liés à la sécurité de l'information		X	

Mesure de sécurité	Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	Risque lié à l'altération de visualisations sans pouvoir la détecter	Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
Assurance multirisque professionnelle et sur les matériels informatiques		X					ORG – Organisation du cabinet	14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité			X
Extension de l'assurance aux risques d'altération d'informations	X		X		X	X	ORG – Organisation du cabinet	14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité			X
Extension de l'assurance aux risques de vol d'informations		X		X			ORG – Organisation du cabinet	14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité			X
Établissement de la liste des exigences réglementaires	X	X	X	X	X		ORG – Organisation du cabinet	15.1. Conformité avec les exigences légales	X		
Signalement systématique des événements de sécurité de l'information par les partenaires	X	X	X	X	X	X	ORG – Partenaire	13.1. Signalement des événements et des failles liés à la sécurité de l'information		X	
Rangement systématique des documents liés aux plans et calculs de structures dans un meuble fermé à clef				X			PAP – Support papier	7.1. Responsabilités relatives aux biens		X	
Rangement des documents de sécurité de l'information dans un meuble fermé à clef	X	X	X	X	X	X	PAP – Support papier	7.1. Responsabilités relatives aux biens		X	
Marquage du besoin de confidentialité des documents papiers liés à la sécurité de l'information	X	X	X	X	X	X	PAP – Support papier	7.2. Classification des informations	X		
Marquage du besoin de confidentialité des documents papiers liés aux devis		X		X			PAP – Support papier	7.2. Classification des informations	X		
Rangement systématique		X					PAP –	10.7. Manipulation des	X		

Mesure de sécurité	Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	Risque lié à l'altération de visualisations sans pouvoir la détecter	Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	Bien support sur lequel elle repose	Thème ISO 27002	Prévention	Protection	Récupération
des documents liés aux devis dans un meuble fermé à clef							Support papier	supports			
Destruction des documents sensibles lors de leur mise au rebut		X		X			PAP – Support papier	10.7. Manipulation des supports	X		
Utilisation de mots de passe de qualité pour chaque compte administrateur	X	X	X	X	X	X	PER – Administrateur	11.3. Responsabilités utilisateurs	X		
Sensibilisation régulière des personnels aux risques encourus	X	X	X	X	X	X	PER – Utilisateur	8.2. Pendant la durée du contrat	X		
Formation des personnels aux outils métiers et aux mesures de sécurité	X	X	X	X	X	X	PER – Utilisateur	8.2. Pendant la durée du contrat	X		
Restitution des biens en fin de contrat		X		X			PER – Utilisateur	8.3. Fin ou modification de contrat	X		
Retrait des droits d'accès en fin de contrat	X	X	X	X	X	X	PER – Administrateur	8.3. Fin ou modification de contrat	X		
Utilisation de mots de passe de qualité pour chaque compte utilisateur	X	X	X	X	X		PER – Utilisateur	11.3. Responsabilités utilisateurs	X		
Changement immédiat du mot de passe en cas de compromission	X	X	X	X	X		PER – Utilisateur	11.3. Responsabilités utilisateurs	X		
Verrouillage en cas d'absence		X		X			PER – Utilisateur	11.3. Responsabilités utilisateurs	X		
Signalement systématique des événements de sécurité de l'information par les utilisateurs	X	X	X	X	X	X	PER – Utilisateur	13.1. Signalement des événements et des failles liés à la sécurité de l'information		X	

Ces mesures de sécurité ont été déterminées dans l'objectif de couvrir différents éléments des risques à traiter (vulnérabilités, menaces, sources de menaces, besoins de sécurité ou impacts), d'aborder la plupart des thèmes de l'ISO 27002, de couvrir les différentes lignes de défense (prévention, protection et récupération), et ont été optimisées bien support par bien support.

Les risques résiduels : 6 risques négligeables subsisteront une fois les mesures appliquées

Si les mesures de sécurité précédemment identifiées sont mises en œuvre, alors le niveau des risques jugés comme intolérables ou significatifs peut être ré-estimé comme suit :

Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre

Niveau de risque				
Gravité	1. Négligeable	2. Limitée	**3. Importante**	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	~~3. Forte~~	4. Maximale

Risque lié à la compromission d'un devis au-delà du personnel et des partenaires

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	~~4. Maximale~~

Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres

Niveau de risque				
Gravité	1. Négligeable	2. Limitée	**3. Importante**	~~4. Critique~~
Vraisemblance	**1. Minime**	~~2. Significative~~	3. Forte	4. Maximale

Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	~~4. Maximale~~

Risque lié à l'altération de visualisations sans pouvoir la détecter

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	3. Importante	4. Critique
Vraisemblance	**1. Minime**	~~2. Significative~~	~~3. Forte~~	4. Maximale

Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver

Niveau de risque				
Gravité	1. Négligeable	**2. Limitée**	~~3. Importante~~	4. Critique
Vraisemblance	1. Minime	**2. Significative**	~~3. Forte~~	4. Maximale

En synthèse, les risques résiduels sont donc les suivants :

Risques résiduels	Gravité	Vraisemblance
Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	3. Importante	1. Minime
Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	2. Limitée	2. Significative
Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	3. Importante	1. Minime
Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	2. Limitée	2. Significative
Risque lié à l'altération de visualisations sans pouvoir la détecter	2. Limitée	1. Minime
Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	2. Limitée	2. Significative

Déclaration d'applicabilité : une seule contrainte ne peut être prise en compte

La prise en compte de chaque contrainte identifiée est explicitée comme suit :

Paramètre à prendre en compte	Explication / Justification
Le personnel est utilisateur de l'informatique, mais pas spécialiste	**Pris en compte** Les mesures de sécurité applicables par le personnel ne demandent pas une grande expertise
Le responsable informatique est l'adjoint du directeur, il est architecte de formation	**Pris en compte** Pour certaines mesures de sécurité techniques (ex : installation d'un RAID), il pourra être assisté de prestataires
Le personnel de nettoyage intervient de 7h à 8h	**Non pris en compte** Les horaires doivent correspondrent à ceux du personnel
La réception des clients se fait dans les bureaux des commerciaux, mais des visites ont parfois lieu au bureau d'études	**Pris en compte** Les risques sont réduits si les visiteurs sont accompagnés, le personnel sensibilisé et les documents sensibles rangés
La période de pointe se situant d'octobre à mai, toute action (installation de système de sécurité, formation et sensibilisation) se fera en dehors de cette période	**Pris en compte** La mise en œuvre des mesures de sécurité se fera progressivement, en perturbant le moins possible l'activité
La société a fait un effort important en matière d'informatisation, tout investissement supplémentaire devra être dûment justifié	**Pris en compte** Les mesures de sécurité formalisées n'engendrent pas de gros investissements et les dépenses à prévoir sont pleinement justifiées par les risques qu'elles traitent
Les règles de conception architecturale doivent être respectées	**Pris en compte** Les mesures de sécurité formalisées ne changent pas les pratiques métiers
Des logiciels professionnels du domaine architectural doivent être employés	**Pris en compte** Les mesures de sécurité formalisées ne demandent pas de changer les logiciels
Le cabinet loue deux étages d'un immeuble au centre ville	**Pris en compte** Les mesures de sécurité formalisées s'appliquent au contexte actuel du cabinet
Le cabinet est au voisinage de commerces divers	**Pris en compte** Les mesures de sécurité formalisées s'appliquent au contexte actuel du cabinet
Aucun déménagement n'est planifié	**Pris en compte** Les mesures de sécurité formalisées ne demandent pas de déménagement

Un plan d'action sur 3 ans

Les échelles de valeurs suivantes ont été utilisées pour élaborer le plan d'action :

Difficulté	Coût financier	Terme	Avancement
1. Faible	1. Nul	1. Trimestre	1. Non démarré
2. Moyenne	2. Moins de 1000€	2. Année	2. En cours
3. Élevée	3. Plus de 1000€	3. 3 ans	3. Terminé

Le plan d'action d'@RCHIMED, trié par terme, avancement et coût financier, est établi comme suit :

Mesure de sécurité	Responsable	Difficulté	Coût financier	Terme	Avancement
Mesures du trimestre					
Activation d'une alarme anti-intrusion durant les heures de fermeture	Directeur	1. Faible	1. Nul	1. Trimestre	3. Terminé
Consignes de fermeture à clef des locaux	Directeur	1. Faible	1. Nul	1. Trimestre	3. Terminé
Dispositifs de lutte contre l'incendie	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	3. Terminé
Climatisation	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	3. Terminé
Contrôle d'accès par mot de passe sous MacOS X	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	3. Terminé
Contrôle d'accès par mot de passe sous Windows XP	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	3. Terminé
Accès restreint en entrée (messagerie, services WEB…)	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	3. Terminé
Activation du WPA2	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	3. Terminé
Sauvegarde hebdomadaire sur des disques USB stockés dans un meuble fermant à clef	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	3. Terminé
Installation d'un antivirus sous MacOS X	Directeur adjoint	1. Faible	2. Moins de 1000€	1. Trimestre	3. Terminé
Installation d'un antivirus sous Windows XP	Directeur adjoint	1. Faible	2. Moins de 1000€	1. Trimestre	3. Terminé
Alimentation secourue	Directeur adjoint	1. Faible	2. Moins de 1000€	1. Trimestre	3. Terminé
Contrat de maintenance informatique (intervention sous 4h)	Directeur adjoint	1. Faible	2. Moins de 1000€	1. Trimestre	3. Terminé
Accord sur le niveau de service de l'hébergeur	Directeur adjoint	1. Faible	2. Moins de 1000€	1. Trimestre	3. Terminé
Assurance multirisque professionnelle et sur les matériels informatiques	Directeur	1. Faible	3. Plus de 1000€	1. Trimestre	3. Terminé
Élaboration d'une politique de sécurité de l'information	Directeur adjoint	2. Moyenne	1. Nul	1. Trimestre	2. En cours
Rangement systématique des documents liés aux plans et calculs de structures dans un meuble fermé à clef	Bureau d'études	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Chiffrement des fichiers liés aux plans et calculs de structures à l'aide de certificats électroniques	Bureau d'études	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Création d'empreintes des fichiers liés aux plans et aux calculs de structure	Bureau d'études	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Création d'empreintes des fichiers liés aux visualisations	Bureau d'études	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Soutien de la direction vis-à-vis de la sécurité de l'information	Directeur	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Mise à jour régulière de l'antivirus des serveurs et de sa base de signatures	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Mise à jour régulière de l'antivirus sous Windows XP et de sa base de signatures	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Mise à jour régulière de l'antivirus sous MacOS X et de sa base de signatures	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Sauvegarde du site Internet à chaque mise à jour	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Définition des responsabilités en matière de sécurité de l'information	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Détermination des droits d'accès selon le métier	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Adoption d'une politique de moindre privilège	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Utilisation d'un identifiant unique	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Rangement des documents de sécurité de l'information dans un meuble fermé à clef	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Utilisation de mots de passe de qualité	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré

Mesure de sécurité	Responsable	Difficulté	Coût financier	Terme	Avancement
pour chaque compte administrateur					
Sensibilisation régulière des personnels aux risques encourus	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Retrait des droits d'accès en fin de contrat	Directeur adjoint	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Désactivation des composants inutiles sur MacOS X	Directeur adjoint	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Désactivation des composants inutiles sur le serveur	Directeur adjoint	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Accès uniquement aux services nécessaires	Directeur adjoint	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Désactivation des composants inutiles sur Windows XP	Directeur adjoint	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Création d'empreintes des fichiers sauvegardés du site Internet	Directeur adjoint	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Identification des exigences en matière d'engagement de confidentialité	Directeur adjoint	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Inventaire des biens sensibles	Directeur adjoint	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Mise en place d'un système de vérification d'intégrité du site Internet	Directeur adjoint	3. Élevée	1. Nul	1. Trimestre	1. Non démarré
Signalement systématique des événements de sécurité de l'information par les partenaires	Directeur adjoint et partenaires	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Enregistrement systématique des visiteurs	Secrétariat	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Utilisation du mode "corrections apparentes" lors des échanges lors de l'établissement des devis	Service commercial	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Sauvegarde immédiate des fichiers liés aux devis sur des disques USB stockés dans un meuble fermant à clef	Service commercial	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Limitation des informations sensibles sur les ordinateurs portables	Service commercial	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Rangement systématique des documents liés aux devis dans un meuble fermé à clef	Service commercial	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Chiffrement des fichiers liés aux devis à l'aide de certificats électroniques	Service commercial	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Création d'empreintes des fichiers liés aux devis	Service commercial	2. Moyenne	1. Nul	1. Trimestre	1. Non démarré
Interdiction d'accès aux locaux à toute personne (dont le personnel de nettoyage) sans la présence de membres du personnel	Tous	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Rangement des supports amovibles dans un meuble fermant à clef	Tous	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Accompagnement systématique des visiteurs dans les locaux	Tous	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Signature d'un engagement de confidentialité par les personnels	Tous	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Restitution des biens en fin de contrat	Tous	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Utilisation de mots de passe de qualité pour chaque compte utilisateur	Tous	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Changement immédiat du mot de passe en cas de compromission	Tous	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Verrouillage en cas d'absence	Tous	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Signalement systématique des événements de sécurité de l'information par les utilisateurs	Tous	1. Faible	1. Nul	1. Trimestre	1. Non démarré
Installation d'un antivirus sur les serveurs	Directeur adjoint	1. Faible	2. Moins de 1000€	1. Trimestre	1. Non démarré
Utilisation d'antivols pour les ordinateurs portables	Service commercial	1. Faible	2. Moins de 1000€	1. Trimestre	1. Non démarré
Utilisation de films empêchant l'espionnage de l'écran des ordinateurs portables	Service commercial	1. Faible	2. Moins de 1000€	1. Trimestre	1. Non démarré
Destruction des documents sensibles lors de leur mise au rebut	Tous	1. Faible	2. Moins de 1000€	1. Trimestre	1. Non démarré
Pose de barreaux aux fenêtres	Directeur adjoint	1. Faible	3. Plus de 1000€	1. Trimestre	1. Non démarré
Mesures de l'année					
Établissement de la liste des exigences réglementaires	Directeur adjoint	1. Faible	1. Nul	2. Année	1. Non démarré
Test trimestriel des fichiers sauvegardés	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré
Vérification des empreintes des fichiers liés aux devis de manière régulière	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré

Mesure de sécurité	Responsable	Difficulté	Coût financier	Terme	Avancement
Journalisation des événements informatiques (accès, erreurs…)	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré
Restriction des accès nécessaires pour la maintenance	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré
Révision de la politique de sécurité de l'information au moins une fois par an	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré
Adoption d'une politique de nommage des fichiers et des versions successives	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré
Contrôle annuel de l'application des mesures de sécurité	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré
Formalisation d'une politique de gestion des mesures cryptographiques (chiffrement, création d'empreintes…)	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré
Marquage du besoin de confidentialité des documents papiers liés à la sécurité de l'information	Directeur adjoint	2. Moyenne	1. Nul	2. Année	1. Non démarré
Conservation de preuves conformément aux dispositions légales	Directeur adjoint	3. Élevée	1. Nul	2. Année	1. Non démarré
Signature d'un engagement de confidentialité par les cotraitants, les clients, la maintenance, le personnel de nettoyage et les partenaires	Directeur adjoint et partenaires	1. Faible	1. Nul	2. Année	1. Non démarré
Marquage du besoin de confidentialité des documents électroniques liés aux devis	Service commercial	2. Moyenne	1. Nul	2. Année	1. Non démarré
Marquage du besoin de confidentialité des documents papiers liés aux devis	Service commercial	2. Moyenne	1. Nul	2. Année	1. Non démarré
Extension de l'assurance aux risques d'altération d'informations	Directeur	2. Moyenne	2. Moins de 1000€	2. Année	1. Non démarré
Extension de l'assurance aux risques de vol d'informations	Directeur	2. Moyenne	2. Moins de 1000€	2. Année	1. Non démarré
Utilisation de scellés sur les ordinateurs afin de pouvoir constater leur ouverture non désirée	Directeur adjoint	1. Faible	2. Moins de 1000€	2. Année	1. Non démarré
Formation des personnels aux outils métiers et aux mesures de sécurité	Directeur adjoint	2. Moyenne	3. Plus de 1000€	2. Année	1. Non démarré
Mesures dans les trois ans					
Gestion des vulnérabilités sur les serveurs	Directeur adjoint	3. Élevée	1. Nul	3. 3 ans	1. Non démarré
Gestion des vulnérabilités sur Windows XP	Directeur adjoint	3. Élevée	1. Nul	3. 3 ans	1. Non démarré
Gestion des vulnérabilités sur MacOS X	Directeur adjoint	3. Élevée	1. Nul	3. 3 ans	1. Non démarré
Établissement d'un accord d'échange d'informations avec les clients et les partenaires	Directeur adjoint et partenaires	2. Moyenne	1. Nul	3. 3 ans	1. Non démarré
Mise en place d'un système RAID logiciel	Directeur adjoint	3. Élevée	3. Plus de 1000€	3. 3 ans	1. Non démarré

Une homologation de sécurité prononcée par le Directeur pour un an

Le Directeur d'@RCHIMED a prononcé l'homologation de sécurité du cabinet au vu de l'étude réalisée (délimitation du périmètre, appréciation des risques, élaboration du plan d'action, mise en évidence des risques résiduels…) et des livrables élaborés (note de cadrage, note de stratégie, politique de sécurité de l'information).

Cette homologation de sécurité est valable un an et pourra être renouvelée tous les ans.

La mise en œuvre du plan d'action devra être démontrée, ainsi que l'amélioration continue de l'étude de sécurité.

3 Livrables

3.1 Note de cadrage (signé par le Directeur)

Suite à la perte récente d'un marché public et avec l'ambition de positionner le cabinet @RCHIMED sur de nouveaux marchés d'envergure, la sécurité de l'information doit aujourd'hui être parfaitement maîtrisée. Il convient de faire face à une rude concurrence tout en maintenant notre grande valeur ajoutée.

Un comité de suivi, composé d'un membre de chaque service et présidé par le Directeur adjoint, réalisera la première étude de risques et se réunira ensuite tous les six mois afin de faire le point sur les évolutions à apporter à la gestion des risques de sécurité de l'information

L'objectif est de gérer les risques SSI sur le long terme et d'élaborer une politique de sécurité de l'information que nous devrons tous appliquer.

Une première réflexion doit être menée, sur 15 jours, et la participation de tout le cabinet est requise, selon la structure de travail suivante :

Activités d'EBIOS	Directeur	Directeur adjoint	Comité de suivi	Secrétariat	Service commercial	Bureau d'études	Service comptabilité	Documents à produire en plus de l'étude des risques	Consignes particulières	Ressources estimées (en h.j)	Durée (en jours)
Activité 1.1 – Définir le cadre de la gestion des risques		R	C	I	I	I	I			2	2
Activité 1.2 – Préparer les métriques		R	C	I	I	I	I		Vérifier l'uniformité de la compréhension	2	2
Activité 1.3 – Identifier les biens	A	R	C	C	C	C	I	Note de cadrage	Ne pas trop détailler	6	2
Activité 2.1 – Apprécier les événements redoutés		R	C	C	C	C	I		Utiliser les bases génériques	6	2
Activité 3.1 – Apprécier les scénarios de menaces		R	C	C	C	C	I		Utiliser les bases génériques	6	2
Activité 4.1 – Apprécier les risques		R	C	I	I	I	I			1	1
Activité 4.2 – Identifier les objectifs de sécurité	A	R	C	I	I	I	I	Note de stratégie		2	1
Activité 5.1 – Formaliser les mesures de sécurité à mettre en œuvre	A	R	C	C	C	C	I	Politique de sécurité de l'information		15	3
Activité 5.2 – Mettre en œuvre les mesures de sécurité	A	R	I	C	C	C	I	Homologation	Cette activité ne sera réalisée de suite	0	0

Légende : R = Réalisation ; A = Approbation ; C = Consultation ; I = Information

Le périmètre d'étude est le sous-ensemble du système d'information du cabinet @RCHIMED correspondant à son cœur de métier :

- gestion des relations commerciales (gestion des devis, projets…) ;
- gestion des études (calculs de structure, plans techniques, visualisations 3D…) ;
- gestion des services web (nom de domaine, site Internet, courrier électronique…).

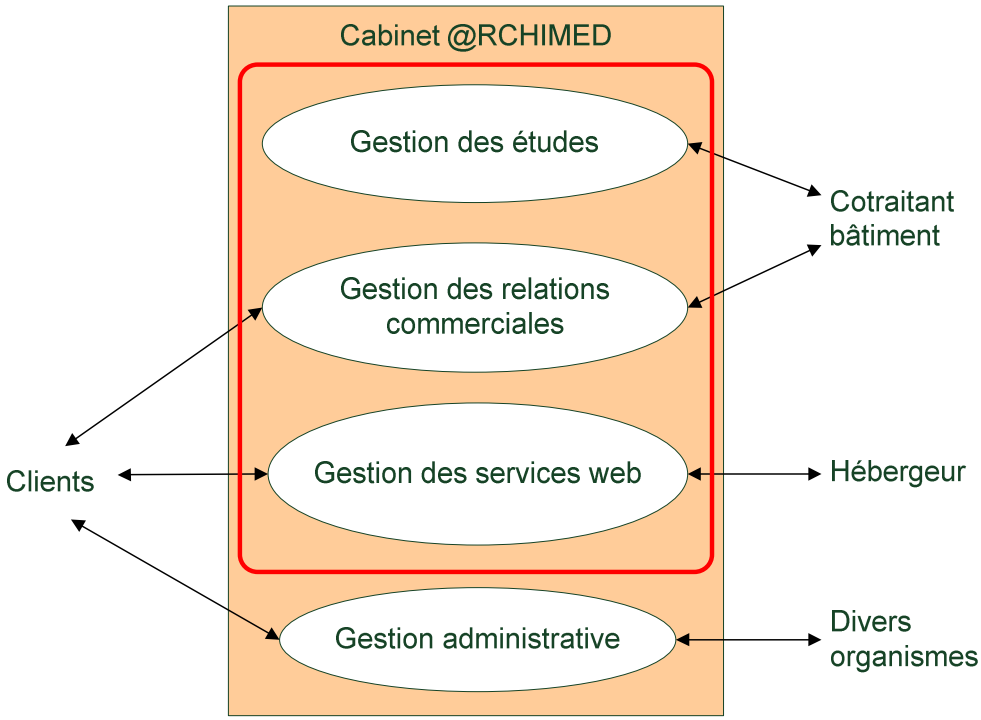

Figure 7 - Le périmètre d'étude

Les enjeux suivants ont été identifiés :

- favoriser l'ouverture du système informatique vers l'extérieur ;
- démontrer la capacité du cabinet à protéger les projets sensibles (assurer la confidentialité relative aux aspects techniques…) ;
- améliorer les services rendus aux usagers et la qualité des prestations ;
- améliorer les échanges avec les autres organismes (fournisseurs, architectes).

Les contraintes à prendre en compte sont les suivantes :

- relatives au personnel :
  - le personnel est utilisateur de l'informatique, mais pas spécialiste,
  - le responsable informatique est l'adjoint du directeur, il est architecte de formation,
  - le personnel de nettoyage intervient de 7h à 8h,
  - la réception des clients se fait dans les bureaux des commerciaux, mais des visites ont parfois lieu au bureau d'études ;
- d'ordre calendaire :
  - la période de pointe se situant d'octobre à mai, toute action (installation de système de sécurité, formation et sensibilisation) se fera en dehors de cette période ;
- d'ordre budgétaire :
  - la société a fait un effort important en matière d'informatisation, tout investissement supplémentaire devra être dûment justifié ;
- d'ordre technique :
  - les règles de conception architecturale doivent être respectées,
  - des logiciels professionnels du domaine architectural doivent être employés ;
- d'environnement :
  - le cabinet loue deux étages d'un immeuble au centre ville,
  - le cabinet est au voisinage de commerces divers,
  - aucun déménagement n'est planifié.

Les sources de menaces retenues sont les suivantes :

- personnel de nettoyage (soudoyé),
- script-kiddies,
- concurrent (éventuellement en visite incognito),
- maintenance informatique,
- employé peu sérieux,
- employé peu sérieux (ceux qui ont un rôle d'administrateur),
- client,
- cotraitant,
- partenaire,
- fournisseur d'accès Internet,
- hébergeur,
- virus non ciblé,
- phénomène naturel (foudre, usure…),
- maladie,
- panne électrique,
- incendie des locaux.

Les critères de sécurité retenus sont la disponibilité, l'intégrité et la confidentialité :

Critères de sécurité	Définitions
Disponibilité	Propriété d'accessibilité au moment voulu des biens essentiels.
Intégrité	Propriété d'exactitude et de complétude des biens essentiels.
Confidentialité	Propriété des biens essentiels de n'être accessibles qu'aux utilisateurs autorisés.

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de disponibilité :

Niveaux de l'échelle	Description détaillée de l'échelle
Plus de 72h	Le bien essentiel peut être indisponible plus de 72 heures.
Entre 24 et 72h	Le bien essentiel doit être disponible dans les 72 heures.
Entre 4 et 24h	Le bien essentiel doit être disponible dans les 24 heures.
Moins de 4h	Le bien essentiel doit être disponible dans les 4 heures.

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes d'intégrité :

Niveaux de l'échelle	Description détaillée de l'échelle
Détectable	Le bien essentiel peut ne pas être intègre si l'altération est identifiée.
Maîtrisé	Le bien essentiel peut ne pas être intègre, si l'altération est identifiée et l'intégrité du bien essentiel retrouvée.
Intègre	Le bien essentiel doit être rigoureusement intègre.

L'échelle suivante sera utilisée pour exprimer les besoins de sécurité en termes de confidentialité :

Niveaux de l'échelle	Description détaillée de l'échelle
Public	Le bien essentiel est public.
Limité	Le bien essentiel ne doit être accessible qu'au personnel et aux partenaires.
Réservé	Le bien essentiel ne doit être accessible qu'au personnel (interne) impliquées.
Privé	Le bien essentiel ne doit être accessible qu'à des personnes identifiées et ayant le besoin d'en connaître.

L'échelle suivante sera utilisée pour estimer la gravité des événements redoutés et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
1. Négligeable	@RCHIMED surmontera les impacts sans aucune difficulté.
2. Limitée	@RCHIMED surmontera les impacts malgré quelques difficultés.
3. Importante	@RCHIMED surmontera les impacts avec de sérieuses difficultés.
4. Critique	@RCHIMED ne surmontera pas les impacts (sa survie est menacée).

L'échelle suivante sera utilisée pour estimer la vraisemblance des scénarios de menaces et des risques :

Niveaux de l'échelle	Description détaillée de l'échelle
1. Minime	Cela ne devrait pas se (re)produire.
2. Significative	Cela pourrait se (re)produire.
3. Forte	Cela devrait se (re)produire un jour ou l'autre.
4. Maximale	Cela va certainement se (re)produire prochainement.

Les critères de gestion des risques retenus sont les suivants :

Action	Critère de gestion des risques (règle choisie pour réaliser l'action)
Expression des besoins (module 2)	✓ Les besoins de sécurité des biens essentiels sont exprimés à l'aide des échelles correspondantes, selon le critère de sécurité étudié.
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 événements redoutés (module 2)	✓ Les événements redoutés sont classés par ordre décroissant de vraisemblance.
Estimation des scénarios de menaces (module 3)	✓ Les scénarios de menaces sont estimés en termes de vraisemblance 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 considéré. ✓ La vraisemblance d'un risque est égale à la vraisemblance maximale de tous les scénarios de menaces liés à l'événement redouté considéré.
Évaluation des risques (module 4)	✓ Les risques dont la gravité est critique, et ceux dont la gravité est importante et la vraisemblance forte ou maximale, sont jugés comme intolérables. ✓ Les risques dont la gravité est importante et la vraisemblance significative, et ceux dont la gravité est limitée et la vraisemblance forte ou maximale, sont jugés comme significatifs. ✓ Les autres risques sont jugés comme négligeables.
Choix de traitement des risques (module 4)	✓ Les risques intolérables doivent être réduits à un niveau acceptable ou transférés, voire évités si cela est possible. ✓ Les risques significatifs devraient être réduits, transférés ou évités. ✓ Les risques négligeables peuvent être pris.
Homologation de sécurité (module 5)	✓ Le traitement des risques ne peut être validé que s'il est démontré que les risques résiduels sont acceptables et que les mesures de sécurité destinées à traiter les risques peuvent être mises en œuvre dans un délai raisonnable.

Le tableau suivant présente les biens supports et leurs liens avec les biens essentiels :

Biens supports \ Biens essentiels	Établir les devis	Créer des plans et calculer les structures	Créer des visualisations	Gérer le contenu du site Internet
Biens supports communs à @RCHIMED				
SYS – Réseau interne	X	X	X	X
MAT – Serveur réseau et fichiers	X	X	X	X
LOG – Serveurs logiciels du réseau interne		X	X	
MAT – Disque USB	X	X	X	
MAT – BOX Wifi	X	X	X	X
MAT – Commutateur	X	X	X	X
MAT – PABX (commutateur téléphonique)	X	X	X	X
MAT – Téléphone fixe	X	X	X	X
MAT – Téléphone portable	X	X	X	X
RSX – Canaux informatiques et de téléphonie	X	X	X	X
ORG – Organisation du cabinet	X	X	X	X
PER – Utilisateur	X	X	X	
PER – Administrateur informatique	X	X	X	X
PAP – Support papier	X	X	X	
CAN – Canaux interpersonnels	X	X	X	X
LOC – Locaux du cabinet	X	X	X	X
Biens supports spécifiques au bureau d'études				
SYS – Sous réseau Ethernet		X	X	
MAT – Ordinateur de design		X	X	
LOG – MacOS X		X	X	
LOG – ARC+ (visualisation)			X	
LOG – Pagemaker (PAO)		X	X	
LOG – Suite bureautique et de messagerie		X	X	
MAT – Ordinateur de calcul et de création		X		
LOG – MacOS X		X		
LOG – SPOT (calculs de résistance)		X		
LOG – Outil de messagerie		X		
LOG – Suite bureautique		X		
RSX – Cordon réseau		X	X	
Biens supports spécifiques aux relations commerciales				
SYS – Sous réseau Wifi	X		X	X
MAT – Ordinateurs portables	X		X	
LOG – Windows XP	X		X	
LOG – Suite bureautique et de messagerie	X		X	
MAT – Ordinateur de mise à jour du site Internet				X
LOG – Windows XP				X
LOG – Logiciel de FTP				X
MAT – Imprimante	X		X	
RSX – Wifi	X		X	X
Partenaires				
SYS – Système de l'hébergeur				X
ORG – Hébergeur				X
SYS – Internet	X			X
ORG – Partenaire	X	X	X	X

L'étude de sécurité doit être réalisée conformément à la présente note de cadrage.

3.2 Note de stratégie (signée par le Directeur)

L'étude de sécurité, réalisée conformément à la note de cadrage, a permis d'établir et de hiérarchiser la liste des risques pesant sur le cabinet @RCHIMED (les risques rayés correspondent à ceux réduits par des mesures de sécurité existantes) :

Gravité					
	4. Critique		✓ Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres		
	3. Importante		✓ Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver	✓ Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre ✓ ~~Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver~~	✓ Risque lié à la compromission d'un devis au-delà du personnel et des partenaires ✓ Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires
	2. Limitée		✓ Risque lié à l'indisponibilité d'un devis au-delà de 72h ✓ Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h ✓ Risque lié à l'indisponibilité de visualisations au-delà de 72h ✓ Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h	✓ ~~Risque lié à l'indisponibilité d'un devis au-delà de 72h~~ ✓ ~~Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h~~ ✓ ~~Risque lié à l'indisponibilité de visualisations au-delà de 72h~~ ✓ Risque lié à l'altération de visualisations sans pouvoir la détecter	✓ ~~Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h~~
	1. Négligeable				✓ Risque lié à la compromission de visualisations, jugées comme publiques ✓ Risque lié à la compromission du contenu du site Internet public
		1. Minime	**2. Significative**	**3. Forte**	**4. Maximale**
		Vraisemblance			

Légende :

Risques négligeables	Risques significatifs	Risques intolérables

Afin de traiter ces risques, les objectifs de sécurité suivants ont été identifiés (les croix correspondent aux premiers choix, les croix entre parenthèses correspondent aux autres possibilités acceptées) :

Risque	Évitement	Réduction	Prise	Transfert
Risque lié à l'indisponibilité d'un devis au-delà de 72h		(X)	X	
Risque lié à l'altération d'un devis qui doit rester rigoureusement intègre	(X)	X	X	(X)
Risque lié à la compromission d'un devis au-delà du personnel et des partenaires	(X)	X	X	(X)
Risque lié à l'indisponibilité de plans ou de calculs de structures au-delà de 72h		(X)	X	
Risque lié à l'altération de plans ou de calculs de structures qui doivent rester rigoureusement intègres	(X)	X	X	(X)
Risque lié à la compromission de plans ou calculs de structures au-delà des personnels et partenaires	(X)	X	X	(X)
Risque lié à l'indisponibilité de visualisations au-delà de 72h		(X)	X	
Risque lié à l'altération de visualisations sans pouvoir la détecter		X	(X)	(X)
Risque lié à la compromission de visualisations, jugées comme publiques		(X)	X	
Risque lié à l'indisponibilité du contenu du site Internet au-delà de 72h		(X)	X	
Risque lié à l'altération du contenu du site Internet sans pouvoir la détecter ni la retrouver		X	(X)	(X)
Risque lié à la compromission du contenu du site Internet public		(X)	X	

Il convient maintenant de déterminer les meures de sécurité qui permettront de satisfaire ces objectifs de sécurité, de proposer un plan d'action et de mettre en évidence l'ensemble des risques résiduels.

3.3 Politique de sécurité de l'information (signée par le Directeur)

Afin de protéger le patrimoine du cabinet @RCHIMED et d'en maîtriser les risques de sécurité de l'information, les règles suivantes doivent être appliquées par les personnes concernées :

Thème	Mesure de sécurité
5.1. Politique de sécurité de l'information	Une politique de sécurité de l'information doit exister
	La politique de sécurité de l'information doit être révisée au moins une fois par an
6.1. Organisation interne	La direction doit soutenir la sécurité de l'information
	Les responsabilités en matière de sécurité de l'information doivent être définies
	Les exigences en matière d'engagement de confidentialité doivent être définies
6.2. Tiers	Les visiteurs dans les locaux doivent être systématiquement accompagnés
	Les visiteurs doivent être systématiquement enregistrés
	Un engagement de confidentialité doit être signé par les cotraitants, les clients, la maintenance, le personnel de nettoyage et les partenaires
7.1. Responsabilités relatives aux biens	Les fichiers liés aux plans et calculs de structures doivent être signés à l'aide de certificats électroniques
	Le mode "corrections apparentes" doit être utilisé lors des échanges lors de l'établissement des devis
	Les fichiers liés aux devis doivent être chiffrés à l'aide de certificats électroniques
	Un inventaire des biens sensibles doit être réalisé
	Une politique de nommage des fichiers et des versions successives doit être adoptée
	Les documents liés aux plans et calculs de structures doivent être systématiquement rangés dans un meuble fermé à clef
	Les documents de sécurité de l'information doivent être rangés dans un meuble fermé à clef
7.2. Classification des informations	Le besoin de confidentialité des documents électroniques liés aux devis doit être marqué
	Le besoin de confidentialité des documents papiers liés à la sécurité de l'information doit être marqué
	Le besoin de confidentialité des documents papiers liés aux devis doit être marqué
8.1. Avant le recrutement	Un engagement de confidentialité doit être signé par les personnels
8.2. Pendant la durée du contrat	Les personnels doivent être sensibilisés régulièrement aux risques encourus
	Les personnels doivent être formés aux outils métiers et aux mesures de sécurité
8.3. Fin ou modification de contrat	Les biens doivent être restitués en fin de contrat
	Les droits d'accès doivent être retirés en fin de contrat
9.1. Zones sécurisées	L'accès aux locaux doit être interdit à toute personne (dont le personnel de nettoyage) sans la présence de membres du personnel
	Des dispositifs de lutte contre l'incendie doivent être mis en place
	Des barreaux doivent être posés aux fenêtres
	Une alarme anti-intrusion doit être activée durant les heures de fermeture
	Les locaux doivent être fermés à clef en cas d'absence de personnels
9.2. Sécurité du matériel	Une climatisation doit être installée
	Des antivols doivent être utilisés pour les ordinateurs portables

Thème	Mesure de sécurité
	Des films empêchant l'espionnage de l'écran des ordinateurs portables doivent être utilisés
	Une alimentation secourue doit être installée
	Des scellés doivent être utilisés sur les ordinateurs afin de pouvoir constater leur ouverture non désirée
	Un contrat de maintenance informatique (intervention sous 4h) doit être mis en place
10.1. Procédures et responsabilités liées à l'exploitation	Les composants inutiles sur MacOS X doivent être désactivés
	Les composants inutiles sur le serveur doivent être désactivés
	Les composants inutiles sur Windows XP doivent être désactivés
10.2. Gestion de la prestation de service par un tiers	Un accord sur le niveau de service de l'hébergeur doit être établi
10.4. Protection contre les codes malveillant et mobile	Un antivirus doit être installé sous MacOS X
	Un antivirus doit être installé sur les serveurs
	Un antivirus doit être installé Windows XP
	L'antivirus des serveurs et sa base de signatures doivent être régulièrement mis à jour
	L'antivirus sous Windows XP de sa base de signatures doivent être régulièrement mis à jour
	L'antivirus sous MacOS X et sa base de signatures doivent être régulièrement mis à jour
10.5. Sauvegarde	Les fichiers sauvegardés doivent être testés chaque trimestre
	Le site Internet doit être sauvegardé à chaque mise à jour
	Les fichiers liés aux devis doivent être sauvegardés immédiatement sur des disques USB stockés dans un meuble fermant à clef
	Les données doivent être intégralement sauvegardées chaque semaine sur des disques USB stockés dans un meuble fermant à clef
10.6. Gestion de la sécurité des réseaux	L'accès en entrée (messagerie, services WEB…) doit être restreint
	Le WPA2 doit être activé
10.7. Manipulation des supports	Les supports amovibles doivent être rangés dans un meuble fermant à clef
	Les documents liés aux devis doivent être systématiquement rangés dans un meuble fermé à clef
	Les documents sensibles doivent être détruits lors de leur mise au rebut
10.8. Échange des informations	Un accord d'échange d'informations avec les clients et les partenaires doit être établi
10.9. Services de commerce électronique	In système de vérification d'intégrité du site Internet doit être mis en place
10.10. Surveillance	Les empreintes des fichiers liés aux devis doivent être vérifiées de manière régulière
	Les événements informatiques (accès, erreurs…) doivent être journalisés
11.1. Exigences métier relatives au contrôle d'accès	Les droits d'accès doivent être déterminés selon le métier
11.2. Gestion de l'accès utilisateur	Une politique de moindre privilège doit être adoptée
11.3. Responsabilités utilisateurs	Une empreinte des fichiers liés aux devis doit être créée
	Une empreinte des fichiers liés aux plans et aux calculs de structure doit être créée
	Une empreinte des fichiers liés aux visualisations doit être créée
	Une empreinte des fichiers sauvegardés du site Internet doit être créée
	Des mots de passe de qualité doivent être utilisés pour chaque

Thème	Mesure de sécurité
	compte administrateur
	Des mots de passe de qualité doivent être utilisés pour chaque compte utilisateur
	Le mot de passe doit être immédiatement changé en cas de compromission
	Les sessions doivent être verrouillées en cas d'absence
11.4. Contrôle d'accès au réseau	Seuls les services nécessaires doivent pouvoir être accédés
11.5. Contrôle d'accès au système d'exploitation	Un contrôle d'accès par mot de passe doit être mis en place sous MacOS X
	Un contrôle d'accès par mot de passe doit être mis en place sous Windows XP
	L'identifiant des utilisateurs doit être unique
11.6. Contrôle d'accès aux applications et à l'information	Les accès nécessaires pour la maintenance doivent être restreints
11.7. Informatique mobile et télétravail	Les informations sensibles doivent être limitées sur les ordinateurs portables
12.2. Bon fonctionnement des applications	Un système RAID logiciel doit être mis en place
12.3. Mesures cryptographiques	Une politique de gestion des mesures cryptographiques (chiffrement, création d'empreintes…) doit être formalisée
12.6. Gestion des vulnérabilités techniques	Les vulnérabilités sur les serveurs doivent être gérées
	Les vulnérabilités sur Windows XP doivent être gérées
	Les vulnérabilités sur MacOS X doivent être gérées
13.1. Signalement des événements et des failles liés à la sécurité de l'information	Les événements de sécurité de l'information doivent être systématiquement signalés par les partenaires
	Les événements de sécurité de l'information doivent être systématiquement signalés par les utilisateurs
13.2. Gestion des améliorations et incidents liés à la sécurité de l'information	Les preuves utiles doivent être conservées conformément aux dispositions légales
14.1. Aspects de la sécurité de l'information en matière de gestion de la continuité de l'activité	Une assurance multirisque professionnelle et sur les matériels informatiques doit être souscrite
	Une extension de l'assurance doit couvrir les risques d'altération d'informations
	Une extension de l'assurance doit couvrir les risques de vol d'informations
15.1. Conformité avec les exigences légales	La liste des exigences réglementaires doit être établie
15.3. Prises en compte de l'audit du système d'information	L'application des mesures de sécurité doit être contrôlée chaque année

Ces règles de sécurité seront déclinées en documents d'application quand cela sera nécessaire.

3.4 Homologation de sécurité (prononcée par le Directeur)

Une étude des risques de sécurité de l'information pesant sur le cabinet @RCHIMED a été réalisée conformément à la note de cadrage et un ensemble de mesures de sécurité a été déterminé de manière cohérente avec la note de stratégie.

Les éléments fournis par le Comité de suivi ont permis de rationaliser très clairement la situation et de prendre les décisions nécessaires pour réduire les risques à un niveau acceptable.

J'atteste donc que le projet a bien pris en compte les contraintes opérationnelles établies au départ, que le système et les informations seront protégés conformément aux objectifs de sécurité, et que le système d'information sera apte à réaliser son rôle avec des risques résiduels acceptés et maîtrisés.

Cette homologation est valable pour une durée d'un an afin de permettre la mise en œuvre de la première partie du plan d'action et d'améliorer la sécurité de l'information en continu.