

Exigences de sécurité d'Inria

Prestation en mode SaaS

DSI-SOC

Auteur(s) : RSSI, DSI-SOC
Version : 1.1
Référence :
Diffusion : DSI

Pages : 23

The Inria logo is a stylized, red, cursive script of the word "Inria". It is positioned in the bottom right corner of the page, which has a white background. The logo is written in a fluid, handwritten style with a red color.

SOMMAIRE

1. Généralités.....	7
1.1. OBJET DU DOCUMENT.....	7
1.2. DOCUMENTS DE REFERENCE.....	7
2. Exigences d'ordre organisationnel.....	8
2.1. FONCTIONS ET RESPONSABILITES LIEES A LA SECURITE DE L'INFORMATION	8
2.1.1. ORG-RES-SDO-01 : Sécurité des données	8
2.1.2. ORG-RES-DCP-01 : Données à caractère personnel	8
2.2. ORGANISATION EN MODE PROJET	9
2.2.1. ORG-PRO-MOE-01 : Organisation de la maîtrise d'œuvre	9
2.2.2. ORG-PRO-MOA-01 : Organisation de la maîtrise d'ouvrage	9
2.3. ORG-SPT-SPT-01 : SEPARATION DES TACHES	10
2.4. ORG-SIG-SIG-01 : LA SECURITE DE L'INFORMATION DANS LA GESTION DE PROJET	10
3. Exigences portant sur les mesures de sécurité	11
3.1. ARCHITECTURE DE LA SOLUTION.....	11
3.1.1. MES-ARC-FIA-01 : Fiabilité de l'architecture physique	11
3.1.2. MES-ARC-CAC-01 : Continuité d'activité	11
3.1.3. MES-ARC-RAC-01 : Reprise d'activité.....	11
3.1.4. MES-ARC-ASU-01 : Accès à la solution par les utilisateurs d'Inria	12
3.1.5. MES-ARC-ASA-01 : Accès à la solution par d'autres applications	13
3.1.6. MES-ARC-SUP-01 : Gestion du support aux utilisateurs	13
3.1.7. MES-ARC-DOC-01 : Documentation et formation.....	13
3.2. POLITIQUES DE SECURITE DE L'INFORMATION ET GESTION DU RISQUE.....	14
3.2.1. MES-PSI-PRI-01 : Principes.....	14
3.2.2. MES-PSI-CHA-01 : Charte informatique du prestataire	14
3.2.3. MES-PSI-PSI-01 : Politique de sécurité de l'information	15
3.2.4. MES-PSI-RIS-01 : Appréciation des risques de sécurité.....	15
3.3. SECURITE LIEE AUX RESSOURCES HUMAINES.....	16
3.3.1. MES-SRH-SEL-01 : Sélection des candidats.....	16
3.3.2. MES-SRH-SEN-01 : Sensibilisation, qualification et formations en matière de sécurité de l'information	16
3.3.3. MES-SRH-FIN-01 : Fin ou modification de contrat	16
3.4. SECURITE DE L'INFORMATION.....	16
3.4.1. MES-SEC-CLA-01 : Classement et manipulation de l'information.....	16
3.4.2. MES-SEC-PRO-01 : Protection des données.....	16
3.4.3. MES-SEC-SUP-01 : Suppression des données d'Inria	17
3.5. GESTION DES BIENS.....	17
3.5.1. MES-BIE-INV-01 : Inventaire des biens.....	17
3.5.2. MES-BIE-RES-01 : Restitution des biens	17
3.5.3. MES-BIE-AMO-01 : Gestion des supports amovibles.....	18
3.5.4. MES-BIE-REB-01 : Mise au rebut d'un matériel.....	18
3.5.5. MES-BIE-REC-01 : Recyclage sécurisé du matériel.....	18
3.6. CONTROLE D'ACCES ET GESTION DES IDENTITES	18
3.6.1. MES-ACC-POL-01 : Politiques et contrôle d'accès	19

3.6.2. MES-ACC-ESU-01 : Enregistrement et suppression des utilisateurs	19
3.6.3. MES-ACC-GES-01 : Gestion des droits d'accès	19
3.6.4. MES-ACC-INT-01 : Contrôle d'accès pour le respect d'intégrité ou respect de propriété intellectuelle	19
3.7. CRYPTOLOGIE	20
3.7.1. MES-CRY-MDP-01 : Hachage des mots de passe.....	20
3.7.2. MES-CRY-FLU-01 : Chiffrement des flux.....	20
3.8. SECURITE PHYSIQUE ET ENVIRONNEMENTALE.....	20
3.8.1. MES-PHY-EXT-01 : Protection contre les menaces extérieures et environnementales.....	20
3.8.2. MES-PHY-PER-01 : Périmètre de sécurité physique	21
3.8.3. Contrôle physique des accès	21
3.8.4. MES-PHY-TRA-01 : Travail dans les zones sécurisées	22
3.8.5. MES-PHY-LIV-01 : Zones d'accès public de livraison et de chargement	23
3.9. SECURITE LIEE A L'EXPLOITATION	23
3.9.1. MES-EXP-PRO-01 : Procédures d'exploitation documentées	23
3.9.2. MES-EXP-CHG-01 : Gestion des changements.....	23
3.9.3. MES-EXP-SEP-01 : Séparation des environnements.....	23
3.9.4. MES-EXP-MAL-01 : Mesures contre les codes malveillants.....	23
3.9.5. MES-EXP-SAV-01 : Sauvegarde des informations.....	24
3.9.6. MES-EXP-JOU-01 : Journalisation des événements.....	24
3.9.7. MES-EXP-PJO-01 : Protection de l'information journalisée	24
3.9.8. MES-EXP-HOR-01 : Synchronisation des horloges.....	24
3.9.9. MES-EXP-VUL-01 : Gestion des vulnérabilités techniques	24
3.10. MES-REV-REV-01 : REVERSIBILITE	24
3.11. SECURITE DES OPERATIONS.....	25
3.11.1. MES-OPE-PRO-01 : Politique de sécurité et procédures de traitement et d'échange d'information.....	25
3.11.2. MES-OPE-CLO-01 : Politique de cloisonnement.....	25
3.11.3. MES-OPE-RES-01 : Mesures sur les réseaux et les systèmes.....	26
3.11.4. MES-OPE-SER-01 : Sécurité des services.....	26
3.12. ACQUISITION, DEVELOPPEMENT ET MAINTENANCE DES SYSTEMES D'INFORMATION.....	26
3.12.1. MES-ADM-POL-01 : Politique de développement sécurisé.....	26
3.12.2. MES-ADM-INT-01 : Environnement sécurisé de développement interne.....	27
3.12.3. MES-ADM-EXT-01 : Développement externalisé	27
3.12.4. MES-ADM-CHG-01 : Procédures de contrôle des changements apportés au système.....	27
3.12.5. MES-ADM-REV-01 : Revue technique des applications après modification de la plateforme d'exploitation.....	27
3.12.6. MES-ADM-PRO-01 : Restrictions relatives aux changements apportés aux logiciels tiers	27
3.12.7. MES-ADM-TES-01 : Phase de test de la sécurité du système.....	27
3.12.8. MES-ADM-DEV-01 : Prise en compte de la sécurité dans les développements.....	28
3.12.9. MES-ADM-PDT-01 : Protection des données de test.....	29
3.13. RELATIONS AVEC DES SOUS-TRAITANTS	29
3.13.1. MES-STR-IDE-01 : Identification des sous-traitants.....	29
3.13.2. MES-STR-ACC-01 : La sécurité dans les accords conclus avec les sous-traitants.....	29
3.13.3. MES-STR-CHG-01 : Gestion du changement avec les sous-traitants.....	29
3.14. GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION.....	30
3.14.1. MES-INC-PRO-01 : Responsabilités et procédures	30
3.14.2. MES-INC-CRI-01 : Gestion de crise.....	31
3.14.3. MES-INC-SIG-01 : Signalement des événements liés à la sécurité de l'information.....	31
3.14.4. MES-INC-REP-01 : Réponse aux incidents liés à la sécurité de l'information.....	32
3.14.5. MES-INC-PRE-01 : Recueil de preuves.....	32

1. Généralités

1.1. OBJET DU DOCUMENT

Ce document décrit les exigences de sécurité d'Inria applicables de manière générale et systématique à toute prestation d'externalisation en mode SaaS pour Inria. Il doit obligatoirement accompagner le modèle de plan d'assurance sécurité (PAS) fourni au prestataire par Inria (qui se réfère au présent document) ou bien le PAS fourni par le prestataire si celui-ci possède une certification du type ISO 27001, afin que le prestataire du marché puisse contractuellement s'engager à mettre en œuvre l'ensemble des mesures nécessaires pour répondre aux exigences de sécurité d'Inria générales et spécifiques au projet d'externalisation.

1.2. DOCUMENTS DE REFERENCE

Le tableau ci-dessous indique les documents applicables et de référence liés à la sécurité.

Nom du document	Origine	Date
PSSI d'Inria	Inria	Juin 2017
Echelle de sensibilité des données https://intranet.inria.fr/Inria/Directions/Direction-generale/Securite-Defense/Echelle-de-sensibilite	Inria	Mars 2020
Guide d'hygiène informatique de l'ANSSI https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/	ANSSI	Sept. 2017
Règlement RGPD	Parlement UE	Mai 2018

2. Exigences d'ordre organisationnel

2.1. FONCTIONS ET RESPONSABILITES LIEES A LA SECURITE DE L'INFORMATION

2.1.1. ORG-RES-SDO-01 : Sécurité des données

Le prestataire doit avoir mis en œuvre et documenté une organisation interne de la sécurité pour assurer la définition, la mise en place et le suivi du fonctionnement opérationnel de la sécurité de l'information au sein de son organisation.

Il doit notamment avoir nommé un responsable de la sécurité des systèmes d'information (RSSI ou toute autre personne exerçant cette fonction) et un responsable de la sécurité physique. Il devra communiquer les coordonnées de son RSSI (ou équivalent) à Inria.

2.1.2. ORG-RES-DCP-01 : Données à caractère personnel

Le prestataire doit définir et attribuer les responsabilités en matière de protection de données à caractère personnel, en cohérence avec son rôle de sous-traitant dans les traitements de données à caractère personnel.

Le prestataire doit désigner un délégué à la protection des données (DPO ou toute autre personne exerçant cette fonction) lorsqu'il traite des données parmi lesquelles figurent des catégories particulières de données à caractère personnel telles que définies dans le RGPD. Il devra communiquer les coordonnées de son DPO (ou équivalent) à Inria.

Le prestataire doit réaliser ou contribuer à la réalisation d'une analyse d'impact relative à la protection des données à caractère personnel lorsque le traitement est susceptible d'engendrer un risque élevé pour les droits et libertés des personnes concernées (traitement de catégories particulières de données à caractère personnel telles que définies dans le RGPD, traitement de données à grande échelle, etc.). Cette analyse doit comporter une évaluation juridique du respect des principes et droits fondamentaux, ainsi qu'une étude plus technique des mesures techniques mises en œuvre pour protéger les personnes des risques pour leur vie privée.

A noter que tout hébergement et transfert de données à caractère personnel d'Inria en-dehors de l'Union Européenne est proscrit par le RGPD.

2.2. ORGANISATION EN MODE PROJET

Cette partie décrit l'organisation à mettre en place à la fois par Inria et par le prestataire pour gérer la sécurité dans le projet d'externalisation.

2.2.1. ORG-PRO-MOE-01 : Organisation de la maîtrise d'œuvre

En tant que maître d'œuvre, le prestataire désignera un interlocuteur responsable de la sécurité, pilotant l'ensemble de la sécurité du projet : sécurité des développements, sécurité du système d'information cible et intégration des composants sécurité. Il est rattaché directement au responsable de l'opération, au directeur de projet par exemple, désigné par le prestataire.

Le responsable de la sécurité désigné par le prestataire prend en charge l'organisation des comités de suivi sécurité (ou toute autre instance traitant des aspects sécurité dans le projet) : convocation, proposition d'ordre du jour, rédaction des comptes-rendus conformément aux clauses spécifiques aux comités de suivi décrites dans le contrat.

Il conseille Inria dans son approche de la sécurité du projet, selon les audits, les incidents perçus sur le système ou les évolutions du contexte opérationnel.

Les coordonnées de ce responsable de la sécurité côté prestataire seront communiquées à Inria dès le début du projet.

2.2.2. ORG-PRO-MOA-01 : Organisation de la maîtrise d'ouvrage

Inria désignera un interlocuteur responsable de la sécurité du projet. Cet interlocuteur unique sera rattaché directement au chef de projet. Cet interlocuteur sera responsable de l'ensemble de la sécurité du projet pour Inria, tant sur les aspects sécurité du système d'information cible que sur les aspects sécurité des interfaces avec le prestataire.

Des réunions du comité de suivi de la sécurité (ou toute autre instance traitant des aspects sécurité dans le projet) seront programmées selon une fréquence telle que décrite dans le plan d'assurance sécurité (PAS). Les participants à ces réunions pour Inria seront au moins le chef du projet, le responsable de la sécurité ainsi que le responsable technique ou fonctionnel lorsqu'ils sont impliqués dans les points à l'ordre du jour.

La sécurité globale du projet repose sur la participation active des différents intervenants : personnel interne qui avait un rôle dans le fonctionnement antérieur du système ou service faisant l'objet de l'opération d'externalisation [intégrateur, développeur, administrateur, exploitant, responsable technique, etc.], maîtrise d'ouvrage et maître d'œuvre.

Le responsable de la sécurité désigné par Inria a pour mission de faciliter les relations entre les différents intervenants, et de mettre à disposition de la maîtrise d'œuvre l'ensemble des documents nécessaires au bon déroulement du projet sécurité lié à l'opération d'externalisation : politique de sécurité interne d'Inria, documentation technique du système [documents d'ingénierie, documents d'exploitation, etc.], spécifications, etc.

Il a également pour mission de s'assurer de la prise en compte globale de la sécurité, par la maîtrise d'ouvrage et la maîtrise d'œuvre.

Il décide de la conduite à tenir selon le résultat des audits, des incidents ou des conseils remontés par le prestataire.

Il valide l'ensemble des actions réalisées au titre de la gestion de la sécurité du projet.

2.3. ORG-SPT-SPT-01 : SEPARATION DES TACHES

Le prestataire doit avoir clairement identifié et documenté les risques associés à des cumuls de responsabilités ou de tâches et avoir prévu le cas échéant des mesures de réduction de ces risques.

2.4. ORG-SIG-SIG-01 : LA SECURITE DE L'INFORMATION DANS LA GESTION DE PROJET

Le prestataire doit avoir procédé préalablement au projet à une estimation des risques pouvant avoir un impact sur le service fourni à Inria, et ce quelle que soit la nature du projet. Cette analyse doit avoir été documentée par le prestataire.

Dans la mesure où un projet affecte ou est susceptible d'affecter le niveau de sécurité du service, le prestataire doit avertir Inria et l'informer par écrit des impacts potentiels, des mesures mises en place pour réduire ces impacts ainsi que des risques résiduels le concernant.

3. Exigences portant sur les mesures de sécurité

3.1. ARCHITECTURE DE LA SOLUTION

Ce chapitre reprend certains des points clés des chapitres qui le suivent.

3.1.1. MES-ARC-FIA-01 : *Fiabilité de l'architecture physique*

Le respect de cette exigence est conditionné par le niveau de service demandé par Inria.

Le prestataire doit avoir mis en œuvre les redondances matérielles nécessaires pour fiabiliser l'architecture physique et ainsi se prémunir des pannes matérielles. Ces redondances interviennent à plusieurs niveaux. Par exemple :

- stockage (ex. : redondance disque, réplication sur une autre baie, etc.) ;
- serveurs physiques (ex. : clustering, déplacement automatique de machine virtuelle d'un hyperviseur à un autre, etc.) ;
- accès réseaux (ex. : redondance des accès, redondance du cœur de réseau comme le fire-wall ou les routeurs) ;
- alimentation électrique (ex : mise en place d'onduleurs électriques, redondance des alimentations électriques).

3.1.2. MES-ARC-CAC-01 : *Continuité d'activité*

Dans le cas où un plan de continuité d'activité (PCA) est demandé par Inria, le prestataire devra avoir mis en place et documenté un tel dispositif incluant les aspects de sécurité.

Le PCA devra notamment prévoir l'organisation et les mesures techniques prévues en cas de crise pour sécuriser l'activité maintenue afin d'assurer un niveau de service suffisant (éventuellement en mode dégradé, à définir avec la maîtrise d'ouvrage d'Inria).

3.1.3. MES-ARC-RAC-01 : *Reprise d'activité*

Dans le cas où un plan de reprise d'activité (PRA) est demandé par Inria, le prestataire devra avoir mis en place et documenté un tel dispositif incluant les aspects de sécurité.

Le PRA devra notamment prévoir l'organisation et les mesures techniques prévues suite à la survenue d'un incident majeur pour sécuriser la remise en activité de la solution.

3.1.4. MES-ARC-ASU-01 : *Accès à la solution par les utilisateurs d'Inria*

Le prestataire devra obligatoirement mettre en place des accès sécurisés à la solution. Par exemple :

- accès direct depuis un navigateur à l'aide de connexions type HTTPS ;
- accès grâce à un VPN ;
- accès via un portail dédié de type reverse-proxy ;
- tunnel chiffré type IPSec entre les infrastructures d'Inria et celles du prestataire.

Des mesures de détection et de protection contre les tentatives d'accès illégitimes à la solution devront avoir été mises en place par le prestataire. Par exemple :

- limitation temporelle des connexions (augmentation du délai de façon exponentielle entre plusieurs tentatives infructueuses de connexion) ;
- blocage temporaire pour une certaine durée du compte après un seuil de tentatives infructueuses ;
- blocage du compte sur lequel une intrusion a été constatée et changement du mot de passe de l'utilisateur ;
- règles de composition des mots de passe à l'état de l'art ;
- détection de plusieurs connexions simultanées du même utilisateur depuis plusieurs adresses IP ;
- détection de plusieurs connexions simultanées d'utilisateurs différents depuis la même adresse IP si ce cas d'usage n'est pas prévu dans l'architecture mise en place ;
- génération d'une alarme en cas de tentative de connexion avec un compte fermé ;
- filtrage automatique ou non des adresses IP sources utilisées pour les tentatives d'intrusions ;
- détection de l'accès d'un utilisateur sans privilèges à des données hors du périmètre normal par exploitation des logs applicatifs détaillés ;
- génération d'une alarme en cas de détection d'un vol de session.

3.1.5. MES-ARC-ASA-01 : Accès à la solution par d'autres applications

Pour une bonne intégration de la solution dans l'ensemble du Système d'Information d'Inria la solution devra pouvoir s'interfacer avec d'autres applications de manière sécurisée (utilisation de protocoles sécurisés, utilisateurs applicatifs et de base de données possédant les droits strictement nécessaire, etc.).

Par exemple, concernant la mise à jour des profils ou des comptes applicatifs présents dans la solution, la solution devra pouvoir être pilotée par les interfaces de synchronisation avec le référentiel des comptes Inria.

Il en est de même pour la constitution et la mise à jour de la base infocentre d'Inria le cas échéant.

3.1.6. MES-ARC-SUP-01 : Gestion du support aux utilisateurs

Dans le cas où une prestation de support fera partie du contrat, le prestataire devra avoir prévu une politique de gestion du support (fonctionnel, technique, administration fonctionnelle) aux utilisateurs mentionnant notamment les aspects sécurité. Par exemple :

- quels outils et modes opératoires sont utilisés pour la prise de contrôle du poste utilisateur à distance ;
- des données à caractère personnel sont-elles manipulées par les équipes de support ;
- s'il y a lieu, quelles précautions sont prises par les équipes de support pour la manipulation de données à caractère personnel ;

3.1.7. MES-ARC-DOC-01 : Documentation et formation

Le prestataire fournira l'ensemble des documentations techniques et fonctionnelles pour décrire l'ensemble des points cités ci-dessus.

3.2. POLITIQUES DE SECURITE DE L'INFORMATION ET GESTION DU RISQUE

3.2.1. MES-PSI-PRI-01 : Principes

Le prestataire doit opérer la prestation à l'état de l'art pour le type d'activité retenu : utiliser des logiciels stables bénéficiant d'un suivi des correctifs de sécurité et paramétrés de façon à obtenir un niveau de sécurité optimal.

Il devra appliquer le guide d'hygiène informatique de l'ANSSI¹ au système d'information du service fourni.

3.2.2. MES-PSI-CHA-01 : Charte informatique du prestataire

Le prestataire devra avoir rédigé une charte informatique décrivant les mesures techniques et organisationnelles qui doivent être mise en œuvre par ses collaborateurs, par exemple :

- seuls les ordinateurs portables du prestataire peuvent être connectés au réseau du prestataire et au réseau d'Inria (avec l'accord explicite d'Inria) ;
- les ordinateurs portables doivent être maintenus à jour et disposer de protections (anti-virus, firewall, etc.) ;
- les ordinateurs portables disposent d'un câble antivol relié à un point d'attache fixe ;
- les disques durs des ordinateurs portables sont systématiquement chiffrés ;
- le personnel disposant de matériel mobile (ordinateur, smartphone, etc.) est sensibilisé à la sécurité des équipements hors site ;
- en cas de sinistre ou de vol de matériel, l'évènement doit être immédiatement et impérativement signalé à la DSI et au RSSI du prestataire ;
- changement de tous les mots de passe des utilisateurs sur les postes infectés.

Dans le cadre du télétravail de ses collaborateurs, le prestataire devra avoir mis en place et documenté des règles de protection sur les matériels hors bureaux.

3.2.3. MES-PSI-PSI-01 : Politique de sécurité de l'information

Le prestataire doit avoir documenté et mis en œuvre une politique de sécurité de l'information identifiant ses engagements quant au respect de la législation et réglementation nationale en vigueur (règlement général sur la protection des données - RGPD², loi 78-17 du 6 janvier 1978 modifiée, etc.) selon la nature des informations qui pourraient lui être confiées par Inria.

Cette politique de sécurité de l'information doit être régulièrement révisée, au moins annuellement ou à chaque changement majeur pouvant avoir un impact sur le service.

¹ Lien : <https://www.ssi.gouv.fr/guide/guide-dhygiene-informatique/>

² Lien : <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>

3.2.4. MES-PSI-RIS-01 : Appréciation des risques de sécurité

Le prestataire doit avoir réalisé et documenté une appréciation des risques de sécurité couvrant l'ensemble du périmètre du service fourni. Cette appréciation de risques devra être faite selon une méthode documentée garantissant la reproductibilité et comparabilité de la démarche (méthode EBIOS, Méhari ou autre).

Le prestataire doit, par exemple, prendre en compte dans l'appréciation des risques :

- la gestion de données d'Inria ayant des besoins de sécurité différents ;
- les risques ayant des impacts sur les droits et libertés des personnes concernées en cas d'accès non autorisé, de modification non désirée et de disparition de données à caractère personnel ;
- les risques de défaillance des mécanismes de cloisonnement des ressources de l'infrastructure technique (mémoire, calcul, stockage, réseau) partagées entre les commanditaires ;
- les risques liés à l'effacement incomplet ou non sécurisé des données stockées sur les espaces de mémoire ou de stockage partagés entre commanditaires, en particulier lors des réallocations des espaces de mémoire et de stockage ;
- les risques liés à l'exposition des interfaces d'administration sur un réseau public.

Lorsqu'il existe des exigences légales, réglementaires ou sectorielles spécifiques liées aux types d'informations confiées par Inria au prestataire, ce dernier doit les prendre en compte dans son appréciation des risques.

Cette appréciation des risques doit être révisée régulièrement, au moins annuellement ou à chaque changement majeur pouvant avoir un impact sur le service.

3.3. SECURITE LIEE AUX RESSOURCES HUMAINES

3.3.1. MES-SRH-SEL-01 : Sélection des candidats

Le prestataire doit disposer d'une procédure de vérification des informations de son personnel pour toute prise de poste (conformément aux lois, aux règlements et à l'éthique).

Note : Ces vérifications doivent être proportionnelles aux exigences métier, à la classification des informations accessibles et aux risques identifiés. À titre d'exemple, le prestataire peut demander au candidat une copie du bulletin n°3 de son casier judiciaire.

3.3.2. MES-SRH-SEN-01 : Sensibilisation, qualification et formations en matière de sécurité de l'information

Les salariés, contractants et utilisateurs tiers du prestataire devront avoir suivi une sensibilisation ou une formation à la sécurité.

3.3.3. MES-SRH-FIN-01 : Fin ou modification de contrat

Le prestataire devra disposer d'une procédure documentée pour le traitement des cessations d'emploi incluant notamment la restitution des dispositifs de contrôle d'accès et du matériel mis à disposition ainsi que la suppression éventuelle des données d'Inria.

3.4. SECURITE DE L'INFORMATION

3.4.1. MES-SEC-CLA-01 : Classement et manipulation de l'information

Le prestataire devra se conformer à l'échelle de sensibilité des données d'Inria pour la mise en œuvre des niveaux de classification de toute information liée au projet et procéder au marquage de cette information.

3.4.2. MES-SEC-PRO-01 : Protection des données

Les données classifiées du projet devront être protégées par le prestataire. Par exemple :

- contrôle de l'intégrité des données (altération, suppression, perte, ...) ;
- détection d'un volume d'échange anormalement élevé qui pourrait être révélateur d'un incident de sécurité portant sur les données tel une exfiltration de données ou un accès illégitime à celles-ci ;
- signalement d'un privilège accordé à une population importante des administrateurs fonctionnels de la solution.

En cas d'incident sur les données du projet, le prestataire devra en informer rapidement le SOC d'Inria (cert@inria.fr) copie RSSI d'Inria (rssi@inria.fr) qui déterminera s'il y a eu – ou pas - une violation de données et si la DPO d'Inria (dpo@inria.fr) doit être prévenue.

3.4.3. MES-SEC-SUP-01 : Suppression des données d'Inria

Au terme du contrat liant le prestataire avec Inria ou en cas de rupture anticipée quelle qu'en soit la cause, ou à la demande d'Inria, l'intégralité des informations d'Inria devra être effacée conformément au délai prévu dans le contrat.

3.5. GESTION DES BIENS

3.5.1. MES-BIE-INV-01 : Inventaire des biens

Biens du prestataire

Le prestataire devra tenir à jour l'inventaire de ses équipements, labellisés selon leur fonction ou le niveau de sensibilité des données présentes sur l'équipement, avec leur localisation.

Biens en lien avec le projet

De même, les biens liés au projet devront être inventoriés au niveau projet ainsi que leur(s) propriétaire(s) :

- biens mis à disposition par Inria (serveurs physiques et virtuels, postes de travail, matériels réseau, imprimantes, logiciels) ;
- liste des données à caractère personnel, sensible ou confidentiel d'Inria avec leurs niveaux de sensibilité respectifs ;
- biens possédés par le prestataire et utilisés dans le cadre du projet.

3.5.2. MES-BIE-RES-01 : Restitution des biens

Biens du prestataire

L'ensemble des salariés, contractants et utilisateurs tiers du prestataire devront restituer la totalité des biens qu'ils ont en leur possession à la fin de leur période d'emploi, contrat ou accord dès lors que des informations d'Inria peuvent être stockées sur ces biens selon une procédure documentée par le prestataire.

Biens en lien avec le projet

Le prestataire devra avoir prévu et documenté une procédure pour la restitution des biens mis à disposition par Inria en n'omettant pas de traiter le cas particulier des données (voir chapitre 3.10 portant sur la réversibilité des données).

3.5.3. MES-BIE-AMO-01 : Gestion des supports amovibles

En cas d'utilisation de supports amovibles dans le cadre du projet il est demandé au prestataire d'avoir prévu et documenté la procédure mise en œuvre pour la gestion des supports amovibles. Cette procédure devra notamment prévoir le chiffrement des données sensibles sur ce type de support.

3.5.4. MES-BIE-REB-01 : Mise au rebut d'un matériel

Le prestataire doit posséder une procédure documentée pour l'effacement sécurisé des données stockées ou leur destruction lors de la mise au rebut d'un matériel.

3.5.5. MES-BIE-REC-01 : Recyclage sécurisé du matériel

Les supports de données appartenant au prestataire et mis au service d'Inria devront être effacés en cas de recyclage.

3.6. CONTROLE D'ACCES ET GESTION DES IDENTITES

Sauf mention explicite, ce chapitre concerne le contrôle d'accès et la gestion des identités des utilisateurs :

- placés sous la responsabilité du prestataire (ses employés et éventuellement des tiers participant à la fourniture du service) ;
- placés sous la responsabilité d'Inria, mais pour lesquels le prestataire met en œuvre les moyens de contrôle d'accès (en fournissant notamment à Inria une interface de gestion des comptes et des droits d'accès).

Les utilisateurs pour lesquels Inria met directement en œuvre les moyens de contrôle d'accès et de gestion des identités sont hors du champ d'application de ce document.

3.6.1. MES-ACC-POL-01 : Politiques et contrôle d'accès

Le prestataire doit avoir mis en place et documenté une politique de gestion des identités et des contrôles d'accès.

Cette politique de gestion des identités et des contrôles d'accès doit être revue périodiquement (au moins annuellement, sauf mention explicite dans le contrat).

3.6.2. MES-ACC-ESU-01 : Enregistrement et suppression des utilisateurs

Une procédure formelle d'enregistrement et de suppression des utilisateurs dans l'outil de gestion des droits d'accès doit exister et être documentée par le prestataire.

3.6.3. MES-ACC-GES-01 : Gestion des droits d'accès

Une procédure permettant de contrôler l'attribution, la modification et la suppression de droits d'accès aux ressources nécessaires à la prestation fournie doit exister et être documentée.

Le prestataire mettra à la disposition d'Inria les outils et les moyens qui permettent une différenciation des rôles des utilisateurs du service, par exemple suivant leur rôle fonctionnel. La liste de tous les utilisateurs ayant accès au service ainsi que le niveau d'autorisation attribué devra être disponible.

Pour chaque utilisateur donné dans le cadre de sa prestation, le prestataire mettra à disposition d'Inria la liste de tous les droits d'accès qu'il a sur les différents éléments du système d'information. Cette liste des droits d'accès des utilisateurs devra être revalidée cycliquement.

3.6.4. MES-ACC-INT-01 : Contrôle d'accès pour le respect d'intégrité ou respect de propriété intellectuelle

L'accès aux paramètres des applications et des programmes, aux binaires et aux codes sources, doit être restreint au personnel autorisé en fonction de la politique de contrôle d'accès (afin de se prévenir de modifications indues).

En outre, l'accès à toute forme de propriété intellectuelle appartenant au prestataire ou à un de ses clients, ainsi que l'utilisation de logiciels propriétaires doit être restreint au personnel autorisé (en fonction de la politique de contrôle d'accès et de licences).

3.7. CRYPTOLOGIE

3.7.1. MES-CRY-MDP-01 : Hachage des mots de passe

En cas de stockage de mots de passe en base, seule l'empreinte des mots de passe devra être stockée avec une méthode de hachage suffisamment robuste. Exemple de fonctions de hachage :

- BCrypt basé sur l'algorithme de chiffrement Blowfish
- scrypt¹ basé sur l'utilisation de PBKDF2² avec la fonction de hachage SHA256³
- Argon2

¹ Voir <https://tools.ietf.org/html/rfc7914>

² <https://tools.ietf.org/html/rfc2898>

³ <https://tools.ietf.org/html/rfc2898>

3.7.2. MES-CRY-FLU-01 : Chiffrement des flux

Les communications réseaux entre le prestataire et Inria feront l'objet d'un chiffrement suffisamment robuste respectant les recommandations décrites dans l'annexe B1 de la version 2 du Référentiel Général de la Sécurité¹.

3.8. SECURITE PHYSIQUE ET ENVIRONNEMENTALE

3.8.1. MES-PHY-EXT-01 : Protection contre les menaces extérieures et environnementales

Le respect de cette exigence est conditionné par le niveau de service demandé par Inria.

Des mesures doivent avoir été mises en place et documentées afin de limiter les risques de départ et de propagation de feu et les risques de dégât des eaux.

Des mesures doivent avoir été mises en place et documentées pour prévenir et limiter les conséquences d'une coupure d'alimentation électrique du site, de la zone ou des salles où sont stockées et traitées les données d'Inria, et permettre une reprise conforme au niveau de disponibilité attendu.

Des moyens de climatisation doivent avoir été mis en place pour maintenir des conditions de température et d'humidité adaptées aux équipements. Des mesures doivent avoir été prises pour prévenir les pannes de climatisation et en limiter les conséquences.

Les équipements de détection et de protection du prestataire doivent être régulièrement contrôlés, testés et maintenus selon des procédures documentées.

3.8.2. MES-PHY-PER-01 : Périmètre de sécurité physique

On nomme ici zones publiques des zones accessibles à tous dans les limites de la propriété du prestataire et n'hébergeant aucune ressource dévolue à l'offre ou permettant d'accéder à des composantes de celle-ci.

On nomme ici zones privées des zones dont les accès sont contrôlés et pouvant héberger :

- a) des plateformes de développement des offres ;
- b) des locaux à partir desquels les intervenants (administrateurs, exploitants, supports) opèrent.

Les zones sensibles sont ici des zones dont les accès sont contrôlés et qui sont réservées à l'hébergement des infrastructures de production et aux moyens d'administration, d'exploitation ou de supervision.

3.8.3. Contrôle physique des accès

3.8.3.1. MES-PHY-PRIV-01 : Zones privées

Les zones privées telles que définies ci-dessus, si présentes dans les locaux du prestataire, doivent être protégées contre les accès non autorisés. En outre, ces zones doivent respecter les exigences suivantes :

- des mesures d'accès dérogatoires en cas d'urgence sont établies et documentées ;

¹ https://www.ssi.gouv.fr/uploads/2014/11/RGS_v-2-0_B1.pdf

- un avertissement relatif aux limites d'accès sur zone doit être affiché à l'entrée des zones privées ;
- les plages horaires d'accès sont déterminées conformément aux besoins des intervenants et précisées dans la politique de sécurité ;
- les visiteurs sont systématiquement accompagnés lors de leurs accès et séjours en zone privée ;
- un dispositif de détection et de surveillance est mis en place et opéré en dehors des heures d'accès autorisées ;
- les pièces inoccupées sont systématiquement verrouillées.

3.8.3.2.MES-PHY-SEN-01 : Zones sensibles

Concernant l'accès aux zones sensibles, si présentes dans les locaux du prestataire, celles-ci doivent être protégées contre les accès non autorisés.

En outre, ces zones doivent respecter les exigences suivantes :

- des mesures d'accès dérogatoires en cas d'urgence sont établies et documentées ;
- un avertissement relatif aux limites d'accès sur zone est affiché à l'entrée des zones sensibles ;
- les plages horaires d'accès sont déterminées conformément aux besoins des intervenants et précisées dans la politique de sécurité ;
- les visiteurs sont systématiquement accompagnés lors de leurs accès et séjours en zone sensible ;
- des dispositifs de détection, de surveillance et de vidéo protection sont mis en place et opérés pendant et en dehors des heures d'accès autorisées ;
- les pièces inoccupées sont systématiquement verrouillées ;
- les accès aux zones sensibles sont systématiquement journalisés et les traces exploitables contrôlées au moins mensuellement.

En cas d'existence de zones sensibles dans les locaux du prestataire, tout accès direct entre une zone publique et une zone sensible devra être évité. Si un tel accès existe, le prestataire devra décrire le mécanisme de sécurisation mis en œuvre.

3.8.4. MES-PHY-TRA-01 : Travail dans les zones sécurisées

Les procédures propres au travail en zone privée ou sensible, si présentes dans les locaux du prestataire, doivent avoir été rédigées et être connues de tous les intervenants concernés.

3.8.5. MES-PHY-LIV-01 : Zones d'accès public de livraison et de chargement

Si les zones de livraison / chargement ou autres sont des points par lesquels des personnes non habilitées peuvent pénétrer dans les locaux, alors elles devront obligatoirement avoir été identifiées par le prestataire comme des zones publiques.

3.9. SECURITE LIEE A L'EXPLOITATION

3.9.1. MES-EXP-PRO-01 : Procédures d'exploitation documentées

Les procédures d'exploitation du prestataire doivent être tenues à jour et accessibles au personnel concerné.

3.9.2. MES-EXP-CHG-01 : Gestion des changements

Une procédure de gestion des changements apportés aux systèmes en production doit exister et être documentée.

Cette procédure doit historiser tout changement ayant un impact sur la sécurité, avec, par exemple, les informations suivantes : date et heure programmées du changement, nature du changement, annonce lors du début et de fin de la mise en place du changement. Cet historique doit être communicable à Inria.

Un système de contrôle / historisation des versions du code source en production doit exister.

3.9.3. MES-EXP-SEP-01 : Séparation des environnements

Les environnements de production doivent obligatoirement être séparés des autres environnements (tests développements, etc.).

3.9.4. MES-EXP-MAL-01 : Mesures contre les codes malveillants

Des mesures de détection, de prévention et de restauration pour se protéger des codes malveillants doivent être mis en œuvre et des procédures ou formations appropriées de sensibilisation des équipes du prestataire mises en place.

3.9.5. MES-EXP-SAV-01 : Sauvegarde des informations

Le prestataire doit avoir prévu et documenté une politique de sauvegarde de la solution fournie (informations, logiciels, configurations, etc.).

3.9.6. MES-EXP-JOU-01 : Journalisation des événements

Un système de journalisation des événements doit être mis en place par le prestataire. Ce système de journalisation doit par exemple prévoir l'enregistrement des activités des utilisateurs (tant au niveau système qu'applicatifs et composants logiciels tels bases de données), les exceptions, les défaillances et les événements liés à la sécurité de l'information.

3.9.7. MES-EXP-PJO-01 : Protection de l'information journalisée

Les équipements de journalisation et les informations journalisées doivent être protégés contre les atteintes à leur disponibilité, intégrité, confidentialité ou traçabilité.

L'accès aux journaux doit être limité à un nombre restreint de comptes (seul ceux ayant besoin de l'information).

3.9.8. MES-EXP-HOR-01 : Synchronisation des horloges

Les horloges des équipements doivent être cohérentes entre elles et l'ensemble des journaux horodatés.

3.9.9. MES-EXP-VUL-01 : Gestion des vulnérabilités techniques

Un processus de veille et de supervision permettant la détection des vulnérabilités techniques de ses systèmes doit avoir été mis en place et documenté par le prestataire.

3.10. MES-REV-REV-01 : REVERSIBILITE

Le candidat s'engagera à apporter l'assistance nécessaire durant la période de migration pour faciliter le transfert des moyens de sécurité matériels et logiciels, et la reprise de leur exploitation par Inria, ou par un autre prestataire de service [cf clause de réversibilité du contrat] ».

3.11. SECURITE DES OPERATIONS

3.11.1. MES-OPE-PRO-01 : Politique de sécurité et procédures de traitement et d'échange d'information

Des politiques, procédures et mécanismes de sécurité pour protéger toutes les opérations qui s'effectuent sur son système d'information doivent avoir été prévues et documentées par le prestataire, par exemple concernant :

- le traitement de l'information qui s'effectue sur les équipements de son système d'information, quel que soit leur type ;
- les échanges d'informations transitant par tous les équipements de télécommunication de son système d'information, quel que soit leur type.

3.11.2. MES-OPE-CLO-01 : Politique de cloisonnement

L'infrastructure du système d'information du prestataire, au niveau système, réseau ou applicatif, doit être conçue, développée, déployée et configurée de manière à gérer du cloisonnement d'un point de vue de la sécurité, par exemple :

- un cloisonnement permettant de séparer le réseau de service et le réseau utilisé pour l'administration et la gestion des services et des ressources ;
- un cloisonnement permettant de séparer les environnements de stockage et de traitement des données de sensibilité différentes.

La politique de sécurité du prestataire décrira précisément pour chaque client ou catégorie de clients les objectifs du cloisonnement mis en œuvre :

- objectif de cloisonnement avec d'autres clients du prestataire dont le niveau de sécurité requis est différent ;
- objectif de cloisonnement avec d'autres clients du prestataire dont le niveau de sensibilité des informations est différent ou non compatible à un hébergement sur une ressource commune ;

- objectif de cloisonnement avec l'environnement du même client pour lequel le niveau de sensibilité des informations est différent ou non compatible à un hébergement sur une ressource commune ;
- objectif de cloisonnement d'un flux par type de flux (flux de données différents).

3.11.3. MES-OPE-RES-01 : Mesures sur les réseaux et les systèmes

Les services, protocoles et ports utilisés doivent être documentés et leur utilisation justifiée.

Dans le cas où des services, protocoles ou ports réputés non sûrs doivent être néanmoins utilisés, le prestataire devra avoir documenté les mesures compensatrices qu'il a mises en place dans une logique de défense en profondeur.

Le prestataire doit avoir prévu et documenté des mesures pour appliquer des techniques de défense en profondeur telles que :

- pour la protection des systèmes (par exemple, durcissement des systèmes d'exploitation, configuration des machines virtuelles, mise en œuvre d'un IPS ou d'un Web Application Firewall en frontal du serveur) ;
- pour la détection et la réponse aux attaques réseaux associées à un comportement anormal du trafic (par exemple, MAC spoofing ou ARP poisoning) et / ou par déni de service (DDoS).

3.11.4. MES-OPE-SER-01 : Sécurité des services

Le prestataire doit avoir identifié et documenté pour tous les services les fonctions, les niveaux de service et les exigences de gestion.

Les spécifications des fonctionnalités réseaux doivent être accessibles à Inria, notamment la capacité et la redondance des réseaux.

3.12. ACQUISITION, DEVELOPPEMENT ET MAINTENANCE DES SYSTEMES D'INFORMATION

3.12.1. MES-ADM-POL-01 : Politique de développement sécurisé

Un cycle de développement formel incluant les étapes d'analyse, de développement, de test doit avoir été mis en place par le prestataire.

Ce cycle de développement doit notamment comporter des procédures pour prévenir ou identifier les failles de sécurité liées au développement du code, comme des revues de sécurité du code.

Le personnel du prestataire doit être régulièrement formé aux bonnes pratiques de développement en terme de sécurité.

3.12.2. MES-ADM-INT-01 : Environnement sécurisé de développement interne

Les environnements de développements et de production mis à disposition d'Inria par le prestataire doivent être séparés et l'environnement de développement sécurisé durant l'intégralité du cycle de développement du système.

3.12.3. MES-ADM-EXT-01 : Développement externalisé

En cas de développement externalisé, le prestataire doit avoir prévu et documenté une procédure de supervision et de contrôle de l'activité de développement déléguée à un (ou des) sous-traitant(s).

3.12.4. MES-ADM-CHG-01 : Procédures de contrôle des changements apportés au système

Le prestataire doit avoir mis en place des contrôles pour se prémunir d'une modification non autorisée sur le code de l'application en production et utiliser un système de gestion de versions.

3.12.5. MES-ADM-REV-01 : Revue technique des applications après modification de la plateforme d'exploitation

En cas de changements apportés aux plateformes d'exploitation le prestataire doit revoir et tester les applications métier critiques afin de vérifier l'absence de tout effet indésirable sur l'activité ou sur la sécurité.

3.12.6. MES-ADM-PRO-01 : Restrictions relatives aux changements apportés aux logiciels tiers

En cas d'utilisation de logiciels tiers, le prestataire ne doit les modifier qu'en cas d'absolue nécessité et dans les limites des accords de licence.

En cas de modification dans un logiciel tiers, celui-ci doit être contrôlé, testé et validé éventuellement par l'éditeur afin de conserver l'intégrité du support et de la maintenance associée.

3.12.7. MES-ADM-TES-01 : Phase de test de la sécurité du système

Les systèmes, nouveaux ou mis à jour pendant les processus de développement, doivent être soumis à un processus de qualification (tests et vérifications) documenté.

3.12.8. MES-ADM-DEV-01 : Prise en compte de la sécurité dans les développements

Le prestataire devra prendre en compte les exigences de sécurité identifiées par Inria au démarrage du projet et communiquées.

Le prestataire devra intégrer dans ses développements les mesures techniques de sécurité nécessaires à la protection contre toute activité frauduleuse, toute divulgation ou modification non autorisée dans la solution lorsque celle-ci sera en exploitation par Inria.

Les équipes de développement du prestataire devront être en mesure de démontrer la mise en œuvre de mesures de sécurité en adéquation avec les exigences du projet.

Le prestataire devra intégrer la démarche de mise en œuvre de la sécurité dans le cycle de vie du projet, en recourant notamment aux pratiques suivantes :

- Prise en compte des mesures de sécurité lors des développements. Par exemple :

- suivi des recommandations de l'OWASP Top 10¹ dans le cadre de projets Web, notamment les risques A1 à A6 et A8 à A10 ;
 - utilisation de frameworks à jour et reconnus ;
 - mise en œuvre de la détection de vols de sessions (par exemple un changement d'adresse IP pour une session active) ;
 - envoi ou affichage d'un message à l'utilisateur après toute action de celui-ci, notamment le positionnement d'habilitations pour lui rappeler ce qu'il vient de mettre en œuvre (quels droits il vient d'accorder sur quel espace à quelles personnes).
- Activités de relectures croisées ou de revues de code, outillées par des composants d'analyse statique de code (ex. SonarQube).
 - Planification d'audits de sécurité, réalisés par le prestataire ou par Inria si souhaité, et donnant lieu à la rédaction d'un rapport d'audit.
 - Sensibilisation des équipes de développement aux bonnes pratiques de l'OWASP et au respect de l'état de l'art notamment en matière de protection des données à caractère personnel.
 - Protection des transactions informatiques afin d'empêcher toute transmission incomplète, erronée ou frauduleuse (données modifiées dans une transaction). Une mesure pour les applications transmettant des données par le réseau consiste à utiliser le protocole TLS pour les transactions mais des mesures complémentaires ou spécifiques peuvent s'avérer nécessaires en fonction des attendus de l'application et des technologies employées.
 - Suivi des vulnérabilités dans le développement : détection, signalement, plan d'action. La découverte d'une faille de sécurité critique sur une application Inria en exploitation doit être immédiatement signalée à Inria par voie sécurisée.

3.12.9. MES-ADM-PDT-01 : Protection des données de test

Les environnements de tests et de développements ne doivent, sauf directive explicite d'Inria, pas contenir de copie des données de la production.

Les données de tests anonymisées (aucun lien possible avec un salarié, un prestataire de service ou tout autre tiers du projet) ou échantillonnées doivent l'être selon un procédé documenté par le prestataire.

En cas de non-respect de la stratégie d'anonymisation des données, le prestataire devra ouvrir un incident sécurité et le remonter à sa DSI et à Inria.

3.13. RELATIONS AVEC DES SOUS-TRAITANTS

3.13.1. MES-STR-IDE-01 : Identification des sous-traitants

Le prestataire devra répertorier l'ensemble des sous-traitants qu'il a identifiés comme participant à la mise en œuvre de l'offre (hébergeur, développeur, intégrateur, archiveur, sous-traitant opérant sur site ou à distance pour les tâches d'administration, etc.).

¹ <https://owasp.org/www-project-top-ten/>

3.13.2. MES-STR-ACC-01 : La sécurité dans les accords conclus avec les sous-traitants

En cas de recours à des sous-traitants, le prestataire devra reporter vers le(s) sous-traitant(s) concerné(s) des exigences de sécurité au moins équivalentes à celles qu'il s'engage à mettre en œuvre dans sa propre politique de sécurité, par exemple au travers d'exigences dans les cahiers des charges ou de clauses de sécurité dans les accords de partenariat. Ces exigences seront contractualisées.

3.13.3. MES-STR-CHG-01 : Gestion du changement avec les sous-traitants

Dans la mesure où un changement de sous-traitant affecte le niveau de sécurité offert à Inria, le prestataire devra en informer Inria.

3.14. GESTION DES INCIDENTS LIES A LA SECURITE DE L'INFORMATION

3.14.1. MES-INC-PRO-01 : Responsabilités et procédures

Le prestataire doit disposer de politiques et procédures documentées pour apporter des réponses rapides et efficaces aux incidents de sécurité. Celles-ci doivent définir les moyens de communication des incidents de sécurité aux clients concernés, et le niveau de sécurité exigé pour cette communication.

Les employés et sous-traitants doivent être informés de ces politiques et de ces procédures et les responsabilités et actions à réaliser doivent être clairement définies pour chaque acteur.

Ces procédures doivent notamment prévoir :

- d'alerter le SOC d'Inria (cert@inria.fr) dès toute suspicion de la survenue d'un incident de sécurité ;
- d'accuser réception dans les 24h à tout incident de sécurité de niveau critique signalé par Inria ;
- d'horodater dans un journal des événements l'ensemble des actions effectuées dans le cadre de la résolution de l'incident (indiquer au moins la date, l'action et les noms des intervenants ayant réalisé l'action) ;
- de présenter des points réguliers de la situation aux interlocuteurs d'Inria (chef de projet, service SOC, RSSI, DPO si incident RGPD) tout au long de la résolution d'un incident critique ;
- de prendre en compte le délai légal de 72h pour une déclaration à la CNIL par la DPO d'Inria dans le cas d'une violation de données personnelles pour fournir à la DPO d'Inria tout renseignements nécessaire (circonstances de l'incident, liste des personnes concernées, données exposées ou détruites, etc.) ;
- de présenter aux interlocuteurs d'Inria (chef de projet, service SOC, RSSI, DPO si incident RGPD) un bilan après résolution de tout incident de sécurité, même non critique ;
- de ne clore l'incident qu'après accord d'Inria lorsque l'incident ne concerne qu'Inria et pas d'autres clients.

3.14.2. MES-INC-CRI-01 : Gestion de crise

Une procédure de gestion de crise prenant en compte les aspects suivants doit avoir été mise en place et documentée par le prestataire :

- a) modalités de déclenchement de crise ;
- b) mise en place de la cellule de crise ;
- c) liste des acteurs et définition de leur rôle ;
- d) déroulement de la crise ;
- e) mise en place d'un canal de communication en interne et avec les clients ;
- f) s'il y a lieu, déclenchement des actions nécessaires à la continuité de l'activité, éventuellement en mode dégradé, pendant l'incident (cf. paragraphe 3.1.2 sur la continuité d'activité) et à la reprise de l'activité après l'incident (cf. paragraphe 3.1.3 sur la reprise d'activité)

Le RSSI d'Inria (rssi@inria.fr) ainsi que le SOC d'Inria (cert@inria.fr) doivent être informés dès le déclenchement de la crise.

3.14.3. MES-INC-SIG-01 : Signalement des événements liés à la sécurité de l'information

Un processus de gestion des incidents de sécurité doit avoir été mis en place et documenté par le prestataire. Ce processus doit notamment prévoir que :

- les incidents seront communiqués au SOC d'Inria (cert@inria.fr) ;
- les incidents de sécurité qualifiés de critiques seront communiqués sans délai au SOC d'Inria (cert@inria.fr) avec copie au RSSI (rssi@inria.fr) et des préconisations faites pour limiter les impacts des incidents détectés ;
- le prestataire exige de ses employés et de ses sous-traitants qu'ils rendent compte de tout incident de sécurité, avéré ou suspecté ;
- le processus mis en place prend en compte la possibilité des clients d'informer le prestataire de tout incident de sécurité, avéré ou suspecté, dans le périmètre de la prestation.

3.14.4. MES-INC-REP-01 : Réponse aux incidents liés à la sécurité de l'information

Des procédures de réponse à incident doivent avoir été mises en place et documentées par le prestataire selon les types d'incidents pouvant se produire, par exemple analyse et remise en état du serveur en cas d'accès par un poste client infecté.

Le prestataire devra informer le SOC d'Inria (cert@inria.fr) de l'état d'avancement et de la résolution de l'incident.

3.14.5. MES-INC-PRE-01 : Recueil de preuves

Des procédures doivent être documentées et des moyens adaptés mis en œuvre par le prestataire pour enregistrer et stocker les informations pouvant servir d'éléments de preuve.