POLITIQUE

Politique de sécurité de l'information

RÉFÉRENCE DOCUMENT :	SG_PSI-Groupe.docx
RÉVISION :	3.0
DATE D'ÉMISSION :	15/03/2024
CLASSIFICATION :	Public
DIFFUSION :	Public

SERMA GROUP - 14, rue Galilée - CS 10055 - 33615 PESSAC Cedex - France
Tél : +33 (0)5 57 26 08 88 | contact@serma.com | www.serma.com
S.A. au capital de 2.301.072 euros | RCS Bordeaux 380 712 828
TVA : FR 65 380 712 828 | CODE APE 7219Z

TABLE DES REVISIONS

Révision	Date	Auteur	Chapitre(s) impacté(s)	Description
2.0	21/09/2022	G. HANNA	Tous	Refonte de la politique
2.1	12/01/2023	M. CIRRI	Tous	Refonte de la politique pour alignement sur la norme ISO27001 :2022
2.2	20/03/2023	M. CIRRI	Tous	Ajout conformité 1.6 et décalage du reste du chapitrage
2.3	02/06/2023	M.CIRRI	Tous	Modifications et corrections de « coquilles »
3.0	15/03/2024	M.CIRRI	2.2.3, 1.7	Mise à jour du titre responsable des données groupe Mise à jour fréquence COPIL SSI Mise à jour de la conformité légale Revue annuelle

RESPONSABLE	VERIFIE PAR	APPROUVE PAR
30/09/2024 X RSSI SERMA Signé par : CIRRI Maxime	26/08/2024 X Directrice Qualité SERMA Signé par : FERRINI Beatrice	X Directeur Général SERMA

TABLE DES MATIERES

1. INTRODUCTION

1.1. Objet du document

L'objectif de ce document est la mise en place d'une Politique de Sécurité de l'Information (notée « PSI » dans le reste du texte) afin d'établir un référentiel dont l'application permettra de répondre aux exigences légales, réglementaires, normatives et contractuelles ainsi qu'aux standards de bonnes pratiques de sécurité de l'information.

La PSI déclinée au sein dudit document définit les règles relatives à l'utilisation des ressources informatiques de SERMA. Elle définit les comportements acceptables et inacceptables au sein de SERMA, les contrôles d'accès et les conséquences potentielles en cas de non-respect des règles. Elle jette également les bases d'une réponse aux incidents en définissant la manière dont les utilisateurs peuvent être surveillés et les mesures qui peuvent être prises en cas de violation de la politique.

Elle doit donc être connue de l'ensemble des acteurs internes, ainsi que, le cas échéant, de l'ensemble des personnes accédant au système d'information de l'organisme (sous-traitants, prestataires, stagiaires…).

Elle doit être prise en compte et strictement respectée par ces derniers, qu'ils exercent des activités pour SERMA ou pour ses clients, dans les locaux de SERMA ou en délégation chez le client.

A ce titre la PSI est un **document général diffusable**.

Il est porté à la connaissance de tous les acteurs suscités.

1.2. Responsabilités

Le Responsable de la Sécurité des Systèmes d'Information (RSSI) est responsable de la définition de cette politique et de ses mises à jour. Il s'engage en la visant à garantir son application.

La Directrice Qualité de SERMA assure la relecture de cette politique, vérifie sa forme et veille à sa cohérence avec les systèmes qualité des filiales.

Le Directeur Général de SERMA valide cette politique au regard de sa pertinence. En la visant, il l'approuve au nom des directions des filiales concernées.

Chaque direction de société SERMA concernée est ensuite responsable du déploiement de cette politique au sein de son organisation.

1.3. Contexte

Dans le cadre de ses activités auprès de ses clients et pour appuyer sa démarche dans la sécurité de l'information SERMA a décidé de s'appuyer sur la norme ISO/IEC 27001:2022 et de viser la certification de l'ensemble de ses activités à l'exception de celles mentionnées en 1.4.3 qui feront l'objet d'une analyse de risque et d'un plan de traitement isolés et spécifiques.

Le contexte de croissance de SERMA et d'acquisitions, étalés sur plusieurs années, l'obligent à déployer de manière progressive cette certification.

Le respect des exigences issues de cette norme permet également de satisfaire aux besoins de sécurité DICT (Disponibilité, Intégrité, Confidentialité, Traçabilité). Une analyse de risque spécifique est en parallèle nécessaire afin d'établir des objectifs de sécurité en cohérence avec les risques identifiés.

1.4. Périmètre

1.4.1. GÉOGRAPHIQUE

Cette politique s'applique à l'ensemble des sites français et au site tunisien de SERMA.

1.4.2. FONCTIONNEL

Cette politique s'applique à l'ensemble des activités des sites concernés de SERMA.

1.4.3. ORGANISATIONNEL

Cette politique s'applique à toutes les sociétés de SERMA à l'exception de :

- Des Business Unit de SERMA SAFETY & SECURITY possédant leur propre système de sécurité (SSL et PASSI),
- SERMA ID MOS,
- PRODUCTIVITY ENGINEERING (localisée en Allemagne).

1.5. Enjeux liés à la sécurité de l'information

La sécurité de l'information doit être en permanence adaptée aux enjeux métiers dans un souci d'efficience combinant l'efficacité des moyens et procédures mis en place avec l'optimisation des coûts de la sécurité.

Cette analyse des enjeux s'appuie sur une évaluation des menaces traduite par une cartographie des risques. Ces derniers peuvent être d'origine accidentelle ou intentionnelle. Ils prennent en compte les impacts métiers pour SERMA en cas de sinistre.

Les enjeux majeurs formalisés ci-dessous sont essentiellement liés aux activités de SERMA, à savoir :

- ✓ Assurer la confidentialité des travaux opérés pour le compte des clients de SERMA,
- ✓ Assurer la confidentialité et l'intégrité des données de SERMA et de ses clients,
- ✓ Garantir le respect des engagements contractuels envers les clients,
- ✓ Renforcer la confiance des clients et valoriser l'image de SERMA,
- ✓ Assurer la conformité légale en termes de sécurité de l'information dans les activités de SERMA concernées,
- ✓ Assurer la gestion des risques par la mise en place de dispositifs organisationnels et techniques adaptés aux besoins des métiers de SERMA,
- ✓ Respecter le principe d'amélioration continue des pratiques de sécurité, le suivi des risques et le maintien d'une organisation pour éviter qu'un évènement redouté ne vienne remettre en cause la disponibilité de l'information dans SERMA,

- ✓ Etablir les infrastructures sécurisées, disponibles et fiables pour assurer la disponibilité de l'information,

Les enjeux précités permettent d'assurer la qualité des services rendus pour les utilisateurs internes et externes, les clients et les partenaires en cohérence avec les besoins de sécurité exprimés.

1.6. Parties intéressées

Les parties intéressées à la PSI de SERMA sont identifiées dans les manuels qualité des entités décrivant leur SMSI.

Elles sont citées à titre d'exemple ci-dessous, le document de référence restant le manuel qualité de l'entité concernée :

- ✓ La direction,
- ✓ Les clients de SERMA,
- ✓ Les fournisseurs et prestataires de SERMA,
- ✓ Les employés de SERMA,
- ✓ Les autorités sur les activités qu'exerce SERMA (CNIL, ..),
- ✓ Les actionnaires de SERMA.

1.7. Conformité

Le tableau ci-dessous répertorie les normes, directives et lois avec des impacts en termes de sécurité de l'information auxquels SERMA doit être conforme :

	Serma Ingenierie	AW2S	Serma Safety and Security	Serma Technologies	ID MOS + PE	Serma Micro-electronics & TFP	Serma Energy
RGPD	X	X	X	X	X	X	X
SAPIN II	X	X	X	X	X	X	X
Loi Informatique et libertés	X	X	X	X	X	X	X
Code des postes et des communications électroniques	X	X	X	X	X	X	X
Loi pour une République numérique	X	X	X	X	X	X	X
ISO27001	X	X	X	X	X	X	X
II901	X		X		X	X	X
LPM 2024 - 2030	En cours d'évaluation						
NIS2			X				

Légende :	
	Applicable dès maintenant
	Applicable à partir de 2024
	Applicable à partir de 2025

1.8. Révision

Cette politique est revue, a minima, annuellement mais aussi à chaque changement majeur de l'organisation.

Si lors de la revue annuelle, celle-ci ne nécessite aucune évolution, l'indice de ce document sera incrémenté de 1 et la table des révisions sera mise à jour comme ci-dessous :

Révision	Date	Auteur	Chapitre(s) impacté(s)	Description
Version. Indice	Date de la revue	Auteur de la revue	Tous	Revue annuelle sans évolution

1.9. Documents de référence

REFERENCE	LIBELLE
ISO/IEC 27001:2022	Technologies de l'information - Techniques de sécurité - Systèmes de management de la sécurité de l'information
ISO/IEC 27002:2022	Information security, cybersecurity and privacy protection — Information security controls
EBIOS RM 2018	EBIOS Risk Manager

2. LE PILOTAGE DE LA PSI SERMA

2.1. Gouvernance

Le pilotage, ou gouvernance, de l'activité de sécurité de l'information de SERMA nécessite la mise en œuvre d'une organisation regroupant les compétences et les instances dédiées à cette dernière. Le but de cette organisation est de valider la politique de sécurité et de contrôler le fonctionnement du système de management de la sécurité de l'information. Cette organisation s'appuie également sur des personnes dont les différents rôles et responsabilités ont pour objectif final la sécurité de l'information au sein de SERMA.

2.2. Les rôles et responsabilités

2.2.1. MATRICE DES RÔLES ET RÉSPONSABILITÉS

Fonctions / Activités	Direction Générale	Direction Met. et Fonc.	RSSI Groupe	Equipes IT	Responsable des données groupe	Utilisateurs SI
Définir le cadre de gestion des risques	C	R	C/A	C	C	I
Identifier, analyser et apprécier les risques et les mesures de traitements appropriées.	C	A	R	C	C	C
Définir les règles et exigences de sécurité et formaliser la PSI	A	C	R	C	C	I
Mettre en œuvre les dispositifs techniques permettant de respecter les exigences	I	I	C/I/A	R	I	I
Contrôler l'application des règles de sécurité	I	I	A	R	I	-
Définir et contrôler la conformité réglementaire sur les données personnelles	I	I	I	I	A/R	-

R : Réalisateur - Met en œuvre l'activité. Il doit y avoir au moins un réalisateur par activité.
A : Approbateur - Garant de la bonne exécution et du résultat de l'activité. Il doit y avoir exactement un approbateur par activité.
C : Contributeur – Est consulté pour contribuer à la bonne réalisation de l'activité.
I : Informé – Est informé du déroulement de l'activité et des résultats.

2.2.2. DIRECTION GÉNÉRALE

La Direction Générale de SERMA, veille à ce que la sécurité du SI soit adaptée aux risques réels et aux enjeux (impact du risque, coût des mesures). Elle s'assure que chaque direction ait déterminé les niveaux de risque acceptables et que les procédures de continuité des activités soient testées et suffisantes pour respecter les engagements et les objectifs métiers. Elle s'engage également à doter l'organisation de la sécurité de l'information des moyens nécessaires à l'atteinte de ces objectifs et à les maintenir dans le temps.

2.2.3. DIRECTION MÉTIER ET FONCTIONNELLE

Les directions métier et fonctionnelles (CEO et COO des filiales de SERMA) déterminent, conjointement avec le RSSI, le risque maximum acceptable de chaque activité dont elles ont la charge. Elles inventorient et classifient ce qu'il est nécessaire de protéger et à quel niveau, et expriment leurs besoins en matière de sécurité. Elles informent le plus rapidement possible le RSSI en cas de situation de risque fort.

Les services des ressources humaines et le service juridique tiennent compte dans leurs missions des aspects législatifs, réglementaires et déontologiques ayant trait à la sécurité du SI. Ils fournissent les informations permettant à chaque collaborateur d'exercer ses responsabilités et s'assurent de l'adéquation entre les dispositifs prévus et les obligations juridiques et réglementaires qui doivent être respectées.

2.2.4. RSSI

Le Responsable de la sécurité des systèmes d'information (RSSI) met en place les moyens nécessaires à la sécurité de l'information de l'entreprise. Ses domaines d'action sont multiples mais ils répondent à un seul objectif : assurer l'intégrité, la cohérence et la confidentialité des données de tous les systèmes d'information de SERMA.

Le RSSI intervient de manière transversale sur l'ensemble du système d'information de SERMA, d'un point de vue organisationnel et technique, en synergie avec les différentes directions.

Son rôle est de :

- ✓ Veiller à l'application de la présente Politique ;
- ✓ Définir un plan d'action sécurité conforme à la Politique de Sécurité, adapté à l'environnement des sociétés de SERMA, couvrant les exigences légales et réglementaires applicables et en assurer le suivi ;
- ✓ Formaliser les documents de sécurité de SERMA, incluant la production du bilan annuel de sécurité ;
- ✓ Quantifier les moyens nécessaires à l'atteinte des objectifs en termes de sécurité de l'information ;
- ✓ Accompagner les métiers et le Délégué à la Protection des Données aux déploiements nécessaires aux protections des données à caractère personnels et sensibles ;
- ✓ Gérer la conformité des traitements et hébergements des données à caractère personnel (applications, sites Web, infrastructure, stockage, …) ;
- ✓ Participer aux activités du Comité de sécurité du SI ;
- ✓ Déployer des campagnes de sensibilisation à la sécurité de l'information ;
- ✓ Veiller à la mise à jour de la Cartographie des Risques de Sécurité Majeurs liés à la sécurité de l'Information ;
- ✓ Réaliser une veille légale, réglementaire et normative en rapport avec la sécurité de l'information ;
- ✓ Garantir la prise en charge des évènements de sécurité ;
- ✓ Inclure un apport d'expertise sécurité aux projets de SERMA;
- ✓ Garantir la mise à jour du tableau de bord de la sécurité.

2.2.5. EQUIPES IT

Equipes IT- Administrateurs SI

Leur rôle est de :

- ✓ Assurer la sécurité des infrastructures réseau et systèmes par la mise en œuvre et la tenue à jour de dispositifs techniques et d'outils de sécurité ;
- ✓ S'assurer du respect des règles et politiques de sécurité ;
- ✓ Assurer la bonne application des plans de sécurité ;
- ✓ Proposer des axes d'améliorations.

Equipes IT – Applicatifs

Quels que soient l'organisation et les rôles définis sur les SI applicatifs dans l'entité, il convient que les activités suivantes soient couvertes pour chaque application existante ou en projet :

Leur rôle est de :

- ✓ Assurer la sécurité de l'application ;
- ✓ S'assurer du respect des règles et politiques de sécurité ;
- ✓ S'assurer de la bonne application des plans de sécurité ;
- ✓ Mettre en œuvre la méthodologie d'intégration de la sécurité dans les projets ;
- ✓ Proposer des axes d'améliorations.

2.2.6. RESPONSIBLE DES DONNÉES PERSONNELLES GROUPE

Le référent informatique et libertés est le référent de la protection des données à caractère personnelles des clients et salariés de.SERMA

Son rôle est de :

- ✓ S'assurer du respect des obligations légales (RGPD, lois nationales) dans les traitements des données à caractère personnel, il est le contact privilégié de la CNIL ;
- ✓ Sensibiliser les collaborateurs dans la collecte, le traitement, l'hébergement, la transmission et la suppression des données à caractère personnelles ;
- ✓ Définir la politique relative aux traitements de données à caractère personnelles ; la décliner en procédures et guides et les partager avec les responsables de traitement ;
- ✓ Être informé en amont (privacy by design) des projets impactant les données à caractère personnelles et accompagner les projets ;
- ✓ S'assurer de la tenue des registres, de leurs mises à jour et piloter des analyses d'impacts ;
- ✓ S'assurer des engagements contractuels des tiers, partenaires et sous-traitants ;

- ✓ Informer la direction groupe et les directions entités régulièrement et les alerter le cas échéant ;
- ✓ Contrôler l'application des réglementations et des procédures par des audits internes.

2.2.7. UTILISATEURS DU SI

Les utilisateurs du SI SERMA représentent l'ensemble des collaborateurs utilisant le SI de SERMA, indépendamment de leur fonction (développeurs, commerciaux, etc..), qu'ils soient internes (employés, stagiaires, intérimaires, etc…) ou externes (prestataires, sous-traitants, tiers, etc…).

Leur rôle est de :

- ✓ Respecter les règles de sécurité de la PSI ;
- ✓ Alerter en cas de suspicion d'un incident de sécurité ;
- ✓ Informer référent informatique et liberté Groupe des violations de sécurité de données à caractère personnel en prenant en compte les obligations de notifications CNIL le cas échéant.

2.3. LA COMITOLOGIE

2.3.1. COMITÉ DE PILOTAGE

D'une fréquence semestrielle, son objectif est de suivre le cadre général dans lequel s'inscrivent la PSI et ses documents d'application. Il coordonne les actions de sécurité transverses. Il procède aux arbitrages majeurs relatifs aux chantiers de la sécurité du SI. Ce comité regroupe les décideurs de l'entreprise ainsi que la DSI. Il se réunit régulièrement afin de valider les différentes évolutions de la PSI. Son fonctionnement est fondé sur un travail participatif visant essentiellement à commenter et valider les travaux relatifs à la sécurité du SI. Le comité de pilotage peut, à sa discrétion, inviter des intervenants tiers pour l'assister dans ses tâches.

2.3.2. COMITÉ DE SÉCURITÉ

D'une fréquence mensuelle, il est composé du RSSI, du Directeur du Système d'Information Groupe ainsi que des membres des équipes IT nécessaires au traitement des sujets à l'ordre du jour de ce comité. Cette instance oriente et suit les chantiers liés à la sécurité opérationnelle de SERMA en veillant à leur cohérence avec les besoins métiers exprimés.

2.3.3. REVUE DE DIRECTION

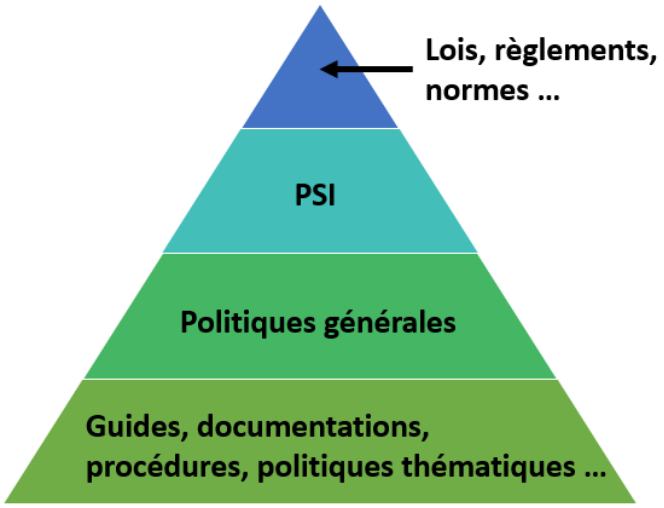
D'une fréquence minimale annuelle, cette revue est en place dans les sociétés de SERMA certifiées ou inscrites dans une démarche ISO 27001. Participent entre autres à cette revue, les directions des sociétés concernées, le RSSI et le DSI. Cette revue permet de :

- ✓ Suivre l'état d'avancement des actions décidées lors des occurrences précédentes ;
- ✓ Prendre en compte et revoir les enjeux internes et externes des parties intéressées pertinentes pour le SMSI ;
- ✓ Réviser, si nécessaire, les besoins et attentes des parties intéressées pertinentes pour le SMSI ;

- ✓ Prendre en compte les retours sur les performances et tendances du SMSI :
  - Suivi des non-conformités et des actions correctives ;
  - Suivi des résultats de la surveillance et du mesurage ;
  - Suivi des résultats des audits ;
  - Suivi de l'atteinte des objectifs en matière de sécurité de l'information ;
- ✓ Prendre en compte les retours des parties intéressées ;
- ✓ Prendre en compte les résultats de l'appréciations des risques et suivre le plan de traitement de ces derniers ;
- ✓ Identifier les opportunités d'amélioration continue.

Le compte-rendu de la revue de direction comporte les décisions relatives aux différents points listés ci-dessus.

2.4. La documentation sécurité



SERMA organise selon le schéma suivant son corpus documentaire

Liste des Politiques générales du SMSI de SERMA :

- POL001 - Gestion de la sécurité
- POL002 - Gestion de la sécurité des actifs et de protection de l'information
- POL003 - Gestion de la sécurité des ressources humaines
- POL004 - Gestion de la sécurité physique
- POL005 - Gestion de la sécurité des systèmes et réseaux
- POL006 - Gestion de la sécurité des applications
- POL007 - Gestion de la sécurité des identités et des accès
- POL008 - Gestion de la sécurité des configurations et des vulnérabilités
- POL009 - Gestion de la sécurité dans la relation avec les fournisseurs
- POL010 - Gestion de la conformité
- POL011 - Gestion des évènements et incidents de sécurité
- POL012 - Gestion de la continuité

Ces documents sont disponibles sur les répertoires dédiés à cet effet du SI de SERMA.

La gestion des révisions et des versions est assurée en remplissant les sections prévues dans la documentation type SERMA.

Révision	Date	Auteur	Chapitre(s) impacté(s)	Description
Version. Indice	Date de la revue	Auteur de la revue	Tous	Revue annuelle sans évolution

2.5. La gestion des risques

SERMA a choisi de se baser sur la méthodologie d'appréciation des risques EBIOS Risk Manager pour réaliser l'analyse des risques liés à la sécurité de l'information.

Les objectifs de cette gestion des risques sont listés ci-dessous :

- ✓ La classification des informations et actifs manipulés ;
- ✓ La conformité aux exigences légales, réglementaires et aux obligations contractuelles qu'il convient d'appliquer ;
- ✓ L'identification des risques à la sécurité de l'information de l'entreprise ;
- ✓ L'évaluation des risques, la probabilité et la gravité des risques identifiés, en prenant en compte les actifs de l'information, les vulnérabilités et les menaces ;
- ✓ La surveillance, l'évaluation et l'approbation des niveaux de risque de sécurité de l'information, en mettant à jour les contrôles, les procédures et les plans de traitement en conséquence.

2.6. L'amélioration continue, les audits et les contrôles

La PSI et sa mise en œuvre fait l'objet d'un contrôle régulier interne et/ou externe (audits). Ces contrôles peuvent porter aussi bien sur des aspects techniques que sur des aspects organisationnels concernant la PSI. Des réunions permettant d'assurer une communauté d'actions entre les différents acteurs de la SSI au sein de SERMA sont organisées régulièrement. Au cours de ces réunions, il est établi un bilan des incidents relevés ainsi que des procédures mises en œuvre. Si nécessaire, il est soumis au comité de pilotage des amendements à la politique de sécurité des systèmes d'information.

Le contrôle permanent est composé de membres indépendants des sociétés de SERMA et supervise notamment les dispositifs permettant de s'assurer :

- ✓ Du suivi de l'ensemble des risques et du niveau de maturité constaté,
- ✓ Du suivi de l'avancement des plans de traitement des risques,
- ✓ Des résultats des mesures et suivis effectués au sein de SERMA,
- ✓ Des incidents rencontrés et des traitements mis en œuvre à la suite d'un incident de sécurité,
- ✓ Des évolutions prévues afin de couvrir les nouveaux risques.

2.7. Les indicateurs du SMSI

Afin de mesurer le niveau de la sécurité de l'information et de piloter l'amélioration continue, un certain nombre d'indicateurs est créé et produit régulièrement.

Leur but est de fournir un état et de surveiller dans le temps la sécurité de l'information.

Leur production est, quand cela est possible, automatisée. Ils doivent fournir des informations pertinentes et être maintenables dans la durée.

3. BONNES PRATIQUES DE LA SECURITE DE L'INFORMATION

Dans le cadre de la sécurité de l'information dans SERMA ce dernier s'engage à respecter à minima les bonnes pratiques listées ci-dessous.

3.1. La sensibilisation de tous à la sécurité de l'information

La sécurité est l'affaire de tous et concourt au bon accomplissement des objectifs métiers de l'entreprise. L'ensemble des employés doit participer régulièrement aux actions de sensibilisation proposées par le RSSI. Des programmes de sensibilisations et de formations sont également proposés en fonction des différents profils de l'entreprise. (CODIR, profils experts et techniques, …)
L'efficacité de ces programmes est testée par la réalisation de questionnaires ou de campagnes globales de vérification de l'efficacité de ces mesures (Tests de Phishing, …)

3.2. Gestion de projet

La sécurité de l'information doit être prise en compte dès la première phase d'étude d'un besoin pour un nouveau projet, pour tous les projets.
Chaque projet doit faire l'objet d'une évaluation de risques pour en évaluer sa criticité. Les responsables de projet doivent s'assurer sur leur périmètre du respect des exigences de sécurité. Dans le cadre d'une prestation externalisée, cette responsabilité revient au responsable de la relation avec le fournisseur.

3.3. Gestion des actifs

Il est indispensable d'identifier les actifs de l'entreprise et d'en définir un responsable.

3.3.1. INVENTAIRE ET PROPRIÉTAIRE D'ACTIF

L'entreprise doit élaborer et maintenir à jour :

- ✓ Une liste de tous ses actifs (postes de travail, serveur, imprimantes, applications et composants tiers, éléments réseaux). Cette dernière doit comprendre l'ensemble des informations permettant de suivre le maintien en conditions opérationnelles et en condition de sécurité des actifs.
- ✓ Un schéma d'architecture logique et physique qui permet de visualiser et de localiser les composants techniques et applicatifs du Système d'Information et leurs interdépendances.

À chaque actif doit être associé un propriétaire chargé de l'inventorier, de le classifier et de le protéger.

3.3.2. MATERIELS ET EQUIPEMENTS SOUS LA RESPONSABILITE DES UTILISATEURS

La charte SI de chaque société encadre l'utilisation et la protection de tout matériel et équipement sous la responsabilité des utilisateurs de SERMA, en vertu de la PSI.

Chaque collaborateur présent au sein des sociétés respectives en prend obligatoirement connaissance et s'engage strictement la respecter.

3.3.3. UTILISATION DES APPAREILS MOBILES

L'utilisation d'appareils mobiles personnels est interdite.

3.3.4. RESTITUTION DES ACTIFS

Une procédure encadrant la restitution des actifs est définie au niveau de SERMA.
Lors du changement de poste, de la cessation de leur contrat ou de leur prestation le personnel de l'entreprise ou le prestataire, doit restituer tous les actifs de l'organisation en sa possession suivant la procédure en place.

3.4. Protection de l'information

Il s'agit de s'assurer que l'information bénéficie d'un niveau de protection approprié afin d'empêcher sa divulgation, sa modification, son retrait ou destruction non autorisée.

3.4.1. UTILISATION DE L'INFORMATION

La procédure de classification de l'information de SERMA encadre l'utilisation et le traitement de l'information. Elle prend en compte tout le cycle de vie de l'information selon sa classification et son marquage.

3.4.2. CLASSIFICATION ET MARQUAGE DE L'INFORMATION

La procédure de classification et manipulation des informations de SERMA encadre la classification des informations et le marquage des documents.
Elle prend en compte exigences légales et réglementaires en matière de confidentialité des informations et de conservation des documents.
Les différentes classifications sont :

- ✓ « Public », information ou document dont la diffusion ne porte pas atteinte à l'image de l'entreprise, ne fournit pas d'avantages concurrentiels ou ne divulgue pas d'informations personnelles sur les collaborateurs de Serma. Cette information peut être accessible et diffusée à tous.
- ✓ « Restreint », information ou document dont la diffusion ne porte pas atteinte à l'image de l'entreprise, ne divulgue pas d'informations personnelles sur les collaborateurs de SERMA mais peut fournir un avantage concurrentiel. Cette information peut être diffusée à tous les collaborateurs et aux personnes externes ayant besoin d'en connaitre.
- ✓ « Confidentiel », information ou document dont la diffusion ne porte pas atteinte à l'image de l'entreprise, mais peut divulguer des informations personnelles sur les collaborateurs de SERMA ou un avantage concurrentiel majeur. Cette information ne doit être diffusée qu'à un ou des groupes de collaborateurs et aux personnes externes ayant besoin d'en connaitre.
- ✓ « Secret », information ou document dont la diffusion porte atteinte à l'image de l'entreprise et dont la diffusion met en danger immédiat la pérennité de l'activité. Cette information ne doit pas être diffusée en dehors de quelques personnes nominativement autorisées.

Le niveau de classification est déterminé par le propriétaire de l'information.
Les documents doivent être marqués avec le niveau de classification de l'information qu'ils contiennent.

3.4.3. TRANSFERT DE L'INFORMATION

La procédure de classification et manipulation des informations de SERMA encadre la gestion et la protection de l'information lors de son transfert.

En cas d'accords dans le cadre de transfert de l'information, il est nécessaire d'établir et de mentionner dans ces accords les politiques, procédures et normes à mettre en œuvre pour la protection des supports physiques et de l'information en transit ; ainsi que les obligations et les responsabilités des parties concernées.

3.4.4. MESSAGERIE

Un système de messagerie sécurisé (contrôle d'accès, configuration des serveurs de messagerie autorisés, bannière légale, transfert automatique / blocage de relais, protocoles, liste de diffusion, traçabilité...) est mis en place et contrôlé. Une analyse et un blocage des contenus malveillants (y compris les pièces jointes) entrants et sortants est mis en place.
Seule la messagerie sécurisée de l'entreprise doit être utilisée à des fins professionnelles. Les adresses de courrier électronique des contractants doivent être différentes de celles des employés. Le niveau de sécurité est le même sur tous les systèmes ou terminaux (poste de travail, smartphone, tablette...) accédant à la messagerie.

3.4.5. PROTECTION CONTRE LES FUITES DE DONNEES

Afin de prévenir et d'empêcher les fuites de données sensibles, SERMA met en place des mesures, appliquées aux systèmes, réseaux et tous appareils qui traitent, stockent ou transmettent des informations sensibles.
Une fois que les données sensibles sont identifiées et classifiées, SERMA décide s'il est nécessaire de restreindre la capacité d'un utilisateur à copier-coller ou télécharger des données vers des services, des appareils et des supports de stockage en dehors de celle-ci.
Le cas échéant, des outils de prévention des fuites de données sont déployés ou les outils existants sont adaptés (email, transfert de fichiers, appareils mobile…) afin d'empêcher l'extraction (soit par copie ou par téléchargement) de données en dehors de son système.
Les outils de prévention des fuites de données permettent d'identifier et surveiller les informations sensibles susceptibles d'être divulguées ; détecter leur divulgation et bloquer les actions des utilisateurs ou les transmissions réseau qui exposent des informations sensibles.

3.5. GESTION DES IDENTITES ET DES ACCES

Il convient de limiter l'accès à l'information et aux moyens de traitement de l'information, de maîtriser l'accès utilisateur par le biais d'autorisations et d'empêcher les accès non autorisés aux systèmes et services d'information.

3.5.1. GESTION DES IDENTITES ET DES ACCES

SERMA dispose d'une procédure de gestion des identités et des accès (revue et gestion des accès).

3.5.2. PROCESSUS FORMEL D'HABILITATION ET D'ACCES AUX RESEAUX ET SERVICES RESEAUX

L'attribution, la modification ou la suppression des droits d'accès doit respecter un processus formel d'habilitation et respecter le besoin d'en connaître.
Seuls les matériels mis à disposition et maitrisés par l'entreprise sont autorisés à se connecter au réseau.

3.5.3. PROTECTION DES COMPTES ET DES MOTS DE PASSE

Une politique de gestion des mots de passe est définie et déployée.

- ✓ La longueur des mots de passe minimale de 12 caractères avec application de règles de complexité (caractères alpha numérique, numérique, caractères spéciaux, chiffres).
- ✓ Le renouvellement des mots de passe.
- ✓ L'historisation des mots de passe.
- ✓ Des mesures pour atténuer les attaques par « Force brute »

Les comptes / mots de passe sont personnels et confidentiels ; ils sont transmis uniquement à l'intéressé et ne doivent pas être communiqués à des tiers.
Les comptes techniques et applicatifs (profil de connexion à la base, compte root …) ne sont connus que par les personnes en ayant besoin.

3.5.4. GESTION DES COMPTES À PRIVILÈGES

L'attribution de comptes à privilèges est restreinte et contrôlée. SERMA réalise une revue périodique des comptes à privilèges.
Les comptes d'administration et d'exploitation sont nominatifs et dédiés à l'administration.

3.5.5. ACCÈS AUX RESSOURCES

L'accès à l'ensemble des ressources sont contrôlés. Seuls les métiers et par délégation les gestionnaires sont autorisés à délivrer les droits d'accès aux systèmes et aux applications.
Tout accès aux systèmes et aux applications est contrôlé par une procédure de connexion sécurisée. L'imputation de toute action sur le SI (hébergé en interne ou en externe) n'est possible que par un identifiant personnel et unique.
Les comptes techniques sont limités et validés. Toute anomalie est contrôlée et corrigée sans délai.

3.5.6. REVUE DES DROITS D'ACCÈS

SERMA réalise des revues des droits d'accès dont la fréquence dépend de la sensibilité.
Tout compte inactif est suspendu puis supprimé avec l'accord du gestionnaire concerné dans un délai raisonnable.

3.6. CONTINUITÉ

SERMA a défini une politique pour la gestion de la continuité d'activité. Elle prend en compte l'ensemble des procédures, dispositifs et moyens mis en œuvre pour permettre de maintenir et restaurer l'activité lors de la survenance d'une crise majeure ou d'un sinistre.

3.6.1. ORGANISATION DE LA CONTINUITE DE LA SECURITE DE L'INFORMATION

SERMA a identifié les besoins de continuité métiers, les scénarios de menaces contre lesquels il doit se prémunir et définit un Plan de Continuité d'Activité (PCA).

3.6.2. ARCHITECTURE TECHNIQUE

SERMA veille à ce que toute architecture technique ou applicative est une documentation d'exploitation complète (incluant le PRI ou PCI).
Le cas contraire cette action est réalisée ou planifiée.
Pour tous les environnements techniques les exigences de dimensionnement sont identifiées afin d'assurer ou d'améliorer leur disponibilité et leur performance.
Le dimensionnement des environnements techniques est surveillé, sa croissance prise en compte et planifiée.

3.6.3. SAUVEGARDES

Une politique et une procédure de gestion des sauvegardes sont définies et déployées. Un plan de sauvegarde et des périodes de rétention sont définis.
Une sauvegarde des données critiques est réalisée et déconnectée du réseau dans un lieu sécurisé.
Une sauvegarde des données critiques est réalisée et stockée à une distance suffisante pour ne pas être atteinte par un sinistre sur le site principal (catastrophe naturelle, incendie, …).
Les matériels et procédures de sauvegarde, restauration et secours sont testés régulièrement (au minimum 1 fois par an).

3.7. SECURITE DES RELATIONS AVEC LES TIERS

SERMA veille au bon niveau de sécurité de l'information et de prestation de services, notamment par le biais d'accords conclus avec les prestataires et s'assure que le niveau de sécurité délivré par le prestataire est adapté à la finalité de la mission ou du service.

3.7.1. ACCORDS CONCLUS AVEC LES PRESTATAIRES ET FOURNISSEURS

Les contrats avec les prestataires et les fournisseurs comportent des mentions relatives à la sécurité de l'information. Il peut s'agir d'un Plan d'Assurance Sécurité (PAS) complété par le prestataire ou le fournisseur et validé par le RSSI groupe ou par le DSI.
D'une manière générale, la PSI et l'ensemble des politiques thématiques de sécurité pertinentes au regard du contexte de la prestation doivent s'appliquer.
Une clause d'audit est intégrée par défaut à l'ensemble des contrats de prestations.

3.7.2. CONNEXION DES TIERS AU RESEAU DE L'ENTREPRISE

Toute connexion de partenaire au réseau de l'entreprise fait l'objet d'une étude particulière validée par le RSSI ou par le DSI.

3.7.3. UTILISATION DES SERVICES CLOUD

SERMA met en œuvre tous les processus d'acquisition, d'utilisation, de gestion et de sortie des services Cloud conformément à ses exigences de sécurité de l'information.
Dans sa stratégie de souveraineté et d'indépendance SERMA s'applique à recourir le moins possible aux services « Cloud ».

3.8. OBLIGATIONS LÉGALES ET CONFORMITÉ

SERMA met en place les processus permettant l'identification et le respect des obligations légales, règlementaires ou contractuelles relatives à la sécurité de l'information.

3.8.1. PROTECTION DE LA VIE PRIVEE ET RGPD

Cette réglementation est bien prise en compte et respectée par SERMA.

Les mesures de conformité prévue sont :

- ✓ La tenue d'un registre des traitements des données personnelles et d'un registre des violations de sécurité des données personnelles ;
- ✓ L'identification des risques spécifiques aux données à caractère personnel ;
- ✓ La formalisation des moyens de protection informatiques et les dispositifs et procédures de traitement des demandes d'exercices de droits par les personnes physiques ;
- ✓ La prise en compte de la protection des données à caractère personnel dès l'étude d'opportunité sur les projets ;
- ✓ La suppression des données qui ne sont plus nécessaires à la finalité des traitements ;

Le responsable des données personnelles de SERMA réalise ou fait réaliser des audits règlementaires périodiquement afin de contrôler la bonne application du RGPD, lois et procédures internes.

3.8.2. VEILLE RÈGLEMENTAIRE

En collaboration avec le RSSI, le DSI, le référent informatique et libertés et la Direction Juridique est maintenu un dispositif de veille réglementaire permettant d'identifier les évolutions légales, normatives ou réglementaires relatives à la sécurité de l'information.

3.8.3. PROPRIÉTÉ INTELLECTUELLE

SERMA s'assure de l'utilisation conforme des logiciels propriétaires et la gestion de leur licence.

3.8.4. CONFORMITÉ À LA PSI

Le RSSI réalise ou fait réaliser des audits fonctionnels et techniques selon un plan d'audit annuel afin de contrôler la bonne application des règles de sécurité de la présente PSI au sein de SERMA.
Le résultat de ces audits est partagé avec les parties prenantes, et fait l'objet d'un plan de recommandations ou de remédiation.

3.9. SÉCURITÉ DES RESSOURCES HUMAINES

Dans le cadre du processus de signature, de rupture ou de modification des termes du contrat de travail, SERMA s'assure que les collaborateurs et contractants comprennent leurs responsabilités et sont compétents pour remplir les fonctions et rôles qui leur sont confiés, ainsi que leur obligation de protéger les intérêts de l'entreprise.

3.9.1. SÉLECTION À L'EMBAUCHE

La vérification des diplômes et certificats professionnels des candidats ainsi que la prise de référence par l'équipe de recrutement est mise en œuvre de façon proportionnée à la sélection des candidats en fonction des responsabilités exercées.

3.9.2. NOUVEAUX ARRIVANTS

Une procédure de gestion des nouveaux arrivants (salariés, stagiaires, prestataires…) existe et permet d'attribuer les ressources standards nécessaires (messagerie, accès au SI) et adaptées à la fonction.

La charte informatique annexée au règlement intérieur de chaque société de SERMA est communiquée aux nouveaux arrivants. Ces derniers doivent en prendre connaissance et l'approuver.

3.9.3. FORMATION ET SENSIBILISATION A LA SSI

Tous les collaborateurs (internes et externes/prestataires) et contractants de SERMA sont sensibilisés une fois par an aux risques liés à la sécurité du SI.
Au travers de ces sensibilisations, SERMA s'assure que tous ses collaborateurs et contractants :

- ✓ Sont responsables de la protection des informations et des systèmes ;
- ✓ Disposent des connaissances, des compétences et outils nécessaires pour appliquer efficacement les règles de sécurité ;
- ✓ Adoptent le comportement attendu en matière de sécurité ;
- ✓ Prennent des décisions efficaces concernant les risques liés aux informations.

Les nouveaux arrivants sont sensibilisés dans les 2 mois suivants leur arrivée.
Par ailleurs, le RSSI communique régulièrement via la messagerie SERMA ou via des newsletters sur les bonnes pratiques en matière de sécurité de l'information.

3.9.4. GESTION DES DÉPARTS

Un dispositif de suivi des sorties (fin de contrat, rupture, fin de stage…) est mis en œuvre permettant l'exécution des mesures de restitution du matériel appartenant à l'entreprise et la fermeture des accès aux systèmes et outils.
Si le besoin le justifie, les accès peuvent néanmoins être maintenus de manière dérogatoire pour une durée limitée.

3.10. NOMADISME

Le télétravail est encadré par la charte dédiée mise en place dans sa société d'appartenance.
SERMA peut toujours réaliser le maintien en conditions de sécurité des équipements de ses collaborateurs en situation de nomadisme numérique.
Les utilisateurs ne doivent ni stocker ni traiter d'information de l'entreprise sur des supports ou terminaux personnels, à l'exception de ceux pour lesquels l'entreprise peut s'assurer de mesures de sécurité minimales et peut effacer à distance les données de l'entreprise.

3.11. SÉCURITÉ PHYSIQUE

SERMA estime qu'il est nécessaire de se prémunir contre toute intrusion dans ses locaux, de prévenir la perte, l'endommagement, le vol ou la compromission des actifs. SERMA se protège également de l'interruption de ses activités, qu'elle soit consécutive à une action volontaire malveillante ou à un incident.

3.11.1. CONTRÔLE D'ACCÈS PHYSIQUE

Les accès aux bâtiments sont restreints uniquement au personnel et aux visiteurs accompagnés.
L'accès aux zones et salles sensibles (salles serveurs, Datacenter) font l'objet d'une sécurité physique supplémentaire permettant de restreindre son accès au personnel autorisé.
Si l'hébergement des données et des infrastructures est laissé à la charge d'un prestataire hébergeur, ces exigences de sécurité lui sont imposées et peuvent être contrôlées.

3.11.2. SÉCURITÉ DU MATÉRIEL

SERMA assure la sécurité physique du matériel et des équipements de l'entreprise. Les bâtiments sont équipés de dispositifs de détection et d'extinction d'incendie.
Les Datacenter ou salles serveurs bénéficient de dispositifs de protection contre les aléas, tels que la surtension ou les inondations pour prévenir tout dommage consécutif à l'un ou l'autre de ces évènements.
À nouveau, si l'hébergement des données et des infrastructures est laissé à la charge d'un prestataire hébergeur, ces exigences de sécurité lui sont imposées et peuvent être contrôlées.

3.11.3. FIN DE VIE ET MISE AU REBUT

Une procédure encadrant la fin de vie et la mise au rebut des actifs est mise en place.
Lors de la destruction, de la restitution ou en cas de réattribution, l'ensemble des supports font l'objet d'un effacement sécurisé, c'est-à-dire en s'assurant de la destruction des données stockées sans possibilité de récupération.

3.12. GESTION DES MENACES ET DES VULNERABILITES

3.12.1. VEILLE ET SIGNALEMENT DES VULNÉRABILITÉS

SERMA met en place une veille sur les vulnérabilités des systèmes d'information.
Toute vulnérabilité probable ou avéré est signalée sans délai et prise en compte.

3.12.2. VEILLE TECHNIQUE SUR LES MENACES

Le RSSI doit mettre en place une veille technique afin de collecter et d'analyser les informations relatives aux menaces et de produire un référentiel à jour de menaces. Ce dernier pourra être utilisé par l'entreprise pour prévenir, détecter ou répondre aux menaces.

3.13. GESTION DES EVENEMENTS LIES A LA SECURITE DE L'INFORMATION

3.13.1. PLANIFICATION ET PREPARATION DE LA GESTION DES INCIDENTS

L'objectif est de garantir une méthode cohérente et efficace de gestion des incidents liés à la sécurité de l'information, incluant la détection, l'instruction et la communication des évènements liés à la sécurité.

SERMA a défini et formalisé une politique et procédure de gestion d'incidents, d'escalade et de crise.
SERMA doit définir et formaliser des scénarios de crise et réaliser un exercice de crise annuel.

3.13.2. SIGNALEMENT DES ÉVÈNEMENTS

Tout évènement lié à la sécurité de l'information (affectant la disponibilité, l'intégrité ou la confidentialité) probable ou avéré est signalé sans délai et pris en compte.

3.13.3. PRISE EN COMPTE ET EVALUATION DES EVENEMENTS

Tout évènement lié à la sécurité de l'information est analysé et classé s'il y a lieu comme incident de sécurité.
L'analyse est encadrée par une procédure formelle qui prend en compte la définition des échelles de classification des incidents.

3.13.4. TRAITEMENT DES INCIDENTS DE SÉCURITÉ

Tout incident de sécurité pouvant avoir un impact significatif sur la sécurité du SI est traité selon la procédure définie et mise en œuvre par SERMA.
Les conclusions d'analyse des évènements et des résolutions d'incidents sont enregistrées en vue de contrôles ou de formalisation d'un référentiel d'incidents liés à la sécurité de l'information.

3.13.5. ACTIVITÉS DE SURVEILLANCE

SERMA met en œuvre un service de centre de contrôle de la sécurité opérationnelle sur ses systèmes.
Les réseaux, les systèmes et les applications sont surveillés pour détecter tout comportement anormal et des mesures appropriées sont prises pour évaluer les incidents potentiels de sécurité des informations.

3.13.6. GESTION DES LOGS

Les capacités de surveillance, de détection et d'alerte sur les événements de sécurité sont définies et mises en œuvre.
Une capacité de détection des comportements anormaux est mise en place et contrôlée en permanence.
Les systèmes en production disposent des logs selon les besoins exprimés par les équipes projets dans une logique de traçabilité.
Les horloges de l'ensemble des systèmes de traitements de l'information sont synchronisées sur une source de temps fiable.

3.14. SÉCURITÉ DES APPLICATIONS

SERMA veille à ce que la sécurité de l'information fasse partie intégrante des Systèmes d'Information tout au long de leur cycle de vie.

3.14.1. ACQUISITION DE NOUVEAUX SYSTÈMES

Tout nouveau système ou mise à jour majeure fait l'objet d'une étude de besoins de sécurité et se conformer aux règles de sécurité de SERMA.

3.14.2. SÉCURITÉ DES APPLICATIONS

Toute application critique est sécurisée dès la phase de conception.

Un contrôle de sécurité systématique est effectué avant toute mise en production afin de garantir la protection de l'intégrité, de la confidentialité et de la disponibilité du SI et de ses données.
Une procédure formelle de gestion et contrôle des changements est suivie pour toutes mise en production.

3.14.3. SÉCURITÉ DES DÉVELOPPEMENTS

SERMA met en œuvre une politique de développement sécurisée.
Elle constitue un ensemble d'exigences permettant de mettre en place un service, une architecture, un logiciel et un système sécurisés.
Les développeurs, internes ou prestataires de SERMA se conforment à minima aux exigences de l'OWASP. Ils évitent l'utilisation de données confidentielles ou de données à caractère personnel à des fins de tests. Dans le cas contraire, la procédure de contrôle d'accès s'applique au système de test et les données immédiatement supprimées après le test effectué.
Les codes source des applications sont sauvegardés sur le serveur de codes sources. Les documents projets sont stockés dans un répertoire sécurisé.
Tout développement donne lieu à une relecture du code par un développeur expérimenté formé au développement sécurisé avant recette et mise en production.
Dans le cas de développement externalisé, SERMA met en place une procédure formelle pour la supervision et le contrôle de cette activité.

3.14.4. SEPARATION DES ENVIRONNEMENTS DE DEVELOPPEMENT, DE TEST ET DE PRODUCTION

Les environnements de développement, de tests et de production sont séparés. Les données de production ne sont pas copiées dans des environnements de tests, à moins que des mesures spécifiques soient mises en œuvre, à savoir, par ordre de préférence :

- ✓ Anonymisation des données de production ;
- ✓ Désensibilisation des données, par isolement d'un échantillon aussi réduit que possible ;
- ✓ Sécurisation de l'environnement de test à un niveau équivalent à l'environnement de production.

3.15. CONFIGURATION SÉCURISÉE

3.15.1. SÉCURITÉ DES POSTES DE TRAVAIL

Les postes de travail font l'objet d'un durcissement conforme aux bonnes pratiques du marché et recommandations, et notamment :

- ✓ La mise en place d'un logiciel de protection contre les logiciels malveillants paramétré par l'équipe informatique et ne pouvant être modifié ou désactivé par l'utilisateur ;
- ✓ Le chiffrement des disques durs des ordinateurs portables ;
- ✓ Les mises à jour de sécurité installées régulièrement ;
- ✓ Le contrôle de la bonne application de la directive de gestion des mots de passe, en particulier quant au renouvellement et à la complexité de ces derniers ;
- ✓ La désactivation des composants et services non nécessaires aux activités ;
- ✓ L'activation du pare-feu local ;
- ✓ L'interdiction d'installer des logiciels tiers non vérifiés ;
- ✓ La suppression des accès administrateurs sur les postes de travail ;
- ✓ Le verrouillage de la session après une période d'inactivité d'au maximum 10 minutes.

3.15.2. USAGE DE LA CRYPTOGRAPHIE

Des moyens cryptographiques sont utilisés pour sécuriser l'accès à l'information, sécuriser l'information elle-même et garantir l'authenticité des échanges.
Des mesures de protection proportionnées sont mises en œuvre pour garantir la sécurité des clés de chiffrement lors de leur stockage et lors de leur utilisation.

3.16. SÉCURITÉ DES SYSTÈMES ET RÉSEAUX

SERMA s'assure de la mise en œuvre de la protection de l'information sur les réseaux et des moyens de traitement de l'information sur lesquels il s'appuie.

3.16.1. PROTECTION DES SERVEURS ET DES VM

Les serveurs hébergeant des données et services, ainsi que les machines virtuelles utilisées dans le cadre des activités d'intégration font l'objet de mesures de protection adaptées à la sensibilité des données, en lien avec l'analyse de risques.
Ces derniers disposent d'un logiciel de protection contre les codes malveillants, d'un suivi des vulnérabilités et des patchs, sont hébergés dans une zone réseau cloisonnée et protégée. Ils font l'objet d'une surveillance et d'une journalisation.
Une revue périodique de la conformité technique des systèmes est planifiée et réalisée.

3.16.2. SÉCURITÉ RÉSEAU

Le système d'information est protégé contre les menaces internes et externes. Les règles d'architecture définissent les zones de sécurité et les échanges autorisés entre ces dernières et l'extérieur du SI.
Le principe de défense en profondeur sont appliqués en mettant en place des réseaux locaux virtuels (VLAN) appropriés, les protocoles sécurisés sont privilégiés lorsque pertinents pour les échanges entre machines (https, sftp, ssh, …).
Le cloisonnement permet, a minima, de séparer les activités métiers des utilisateurs et les environnements d'administration (AD, sauvegarde…).
Les périmètres extérieurs à la zone de confiance sont filtrés par les firewalls.

3.16.3. SÉCURITÉ WIFI

Seuls les réseaux wifi sécurisés (séparation des réseaux, filtrage, contrôle d'accès, profil) validés sont utilisés et surveillés en permanence (flux entrant et sortant) au sein de l'entreprise. Toute connexion wifi doit faire l'objet d'une authentification.

3.16.4. ACCÈS DISTANTS

Tout accès à distance ou en mobilité nécessite une authentification multi-facteur et un tunnel chiffré. Les opérations de maintenance sont pré approuvées, tracées, limitées au minimum nécessaire (durée, type d'accès).

3.16.5. ACCÈS INTERNET

L'authentification est obligatoire et les profils de navigation sur Internet sont définis et contrôlés.

Une surveillance constante des flux entrants et sortants est effectuée pour détecter et bloquer toute utilisation suspecte. Les utilisateurs sont informés explicitement de cette surveillance au préalable dans la charte SI.