OCI INFORMATIQUE & DIGITAL

Politique de sécurité du système d'information – PSSI OCI OUEST – Version Publique

Version 3.1
07/07/2025

Fiche de suivi contacts et des mises à jour du document

Rédacteurs interlocuteurs et évolutions du document :

Pour compléter le document, vous pouvez vous référer à la politique de classification :

Circuit de validation interne OCI OUEST

	Prénom Nom	Fonction	Date
Rédaction	Martial BABILAERE	RSSI	02/01/2025
Approbation	Mathieu LE TORREC	RSMSI	10/01/2025
Validation	Nadège COGARD	RSMQ	07/07/2025

Gestion des changements de version

Version	Date	Objet de la version
V3.1	07/07/2025	Version Public PSSI

Politique de sécurité des systèmes d'information 6
Évolution de la PSSI 6
Diffusion de la PSSI 6
Contrôle d'application de la PSSI 7
Principes organisationnels 8
1. Gouvernance du SMSI 8
Acteurs de la sécurité 9
2. Gestion des risques 9
2.1. Méthodologie EBIOS 9
2.2. Cycle de vie de l'analyse de risque 10
2.3. Sécurité dans les projets 11
3. Protection des informations 12
4. Échelle et critères de détermination des besoins de la sécurité 12
5. Gestion des accès 13
Principe de mise en œuvre 14
1. Aspects humains 14
1.1. Clause de confidentialité 14
1.2. Charte informatique 14
1.3. Charte administrateur 14
1.4. Sélection du personnel qualifié 14
2. Principes généraux d'habilitation 14
3. Redondance des compétences 15
4. Planification de la continuité des activités 15
4.1. Plan de continuité de l'activité 15
4.2. Plan de reprise d'activité 15
5. Gestion des incidents 16
5.1. Caractéristique d'un incident 16
5.2. Dispositifs de détection et d'alerte des incidents 16
5.3. Déclaration et gestion des incidents 16
5.4. Déclaration et gestion d'un problème 17
6. Sensibilisation et formation 17
6.1. Sensibilisation et formation à la sécurité 17
6.2. Communication sur la SSI 17

7. Exploitation 18
7.1. Règle d'utilisation du SI 18
7.2. Documentation des procédures et règles d'exploitation 18
7.3. Conditions applicables à l'infogérance fournie par les filiales de OCI OUEST 18
8. Préventions des vulnérabilités 19
Aspects physiques et environnementaux 20
1. Prévention des menaces environnementale 20
2. Mesures de sécurité physique 20
2.1. Découpage de l'infrastructure en zones de sécurité 20
2.2. Protection contre les accidents et pannes physique. 20
Principes techniques 21
1. Identification / authentification 21
1.1. Utilisation du SSO 21
1.2. Authentification MFA 21
1.3. Séparation des comptes d'utilisation et d'administration 21
1.4. Stratégie de mot de passe 21
1.5. Utilisation d'un gestionnaire de mot de passe 22
1.6. Délivrance et recouvrement des moyens d'authentifications 22
2. Sauvegarde 22
3. Contrôle d'accès logique 23
3.1. Dispositifs et procédures de protection contre les intrusions 23
3.2. Cloisonnement des réseaux et maîtrise des flux 23
4. Modalités d'utilisation sécurisée des réseaux de télécommunication de l'organisme 23
5. Journalisation 24
5.1. Moyens de journalisation communs 24
5.2. Enregistrement des opérations 24
5.3. Alertes de sécurité 24
5.4. Constitution de preuves 24
6. Infrastructures de gestion des clés cryptographiques 25
6.1. Généralité 25
6.2. Algorithmes cryptographiques 25
6.3. Gestion des certificats 25

6.4. Protection des clés 25
7. Signaux compromettants 25
7.1. Généralité 25
7.2. Cages de Faraday 26

Politique de sécurité des systèmes d'information

La Politique de Sécurité des Systèmes d'Information (PSSI) définit les principes généraux de sécurité que la société OCI OUEST a retenu pour s'assurer de disposer d'un système d'information capable de contribuer à l'atteinte de ses objectifs stratégiques.

Cette politique comporte des mesures techniques, mais également nombre de mesures organisationnelles s'adressant au management de l'entreprise, et aux utilisateurs de ce système d'information.

Évolution de la PSSI

OCI OUEST évolue constamment (organisation, missions, périmètre, axes stratégiques, valeurs). Le système d'information (SI) est donc en constante mutation. Par conséquent, la présente politique de sécurité de l'information (PSSI) peut être mise en réexamen par la gouvernance lors des situations suivantes :

- Évolution majeure du contexte ou du SI : Changement d'organisation, adoption de nouvelles technologies, etc.
- Évolution de la menace : Apparition de nouvelles cyberattaques, découverte de failles de sécurité, etc.
- Évolution des besoins de sécurité : Nouvelles exigences réglementaires, besoins accrus en matière de confidentialité, etc.
- À la suite d'un audit : Identification de failles dans la PSSI ou dans sa mise en œuvre.
- À la suite d'un incident de sécurité : Remise en question de l'efficacité des mesures de sécurité en place.
- Systématiquement à intervalle défini : Tous les ans.
- Sur demande d'une autorité : Responsable de la sécurité, direction, etc.

Diffusion de la PSSI

Cette PSSI ainsi que toutes ses déclinaisons opérationnelles sont documentées, versionnées et sont accessibles à tous les personnels.

La présente PSSI doit être connue de l'ensemble des acteurs internes accédant aux systèmes d'information de l'organisme.

La présente PSSI contient un ensemble d'informations diffusables en externe. Une version confidentielle nommée « POLSEC802-PSSI Politique de la sécurité de l'information OCI OUEST » est également disponible pour les besoins internes.

Il est précisé que les informations ci-incluses ne doivent être utilisées que pour connaître le niveau de sécurité mis en place au sein de OCI OUEST. De manière générale, le lecteur s'engage à utiliser le document dans son intégralité et sans modifier son contenu car le document n'a sa cohérence que lorsqu'il est intégral.

Par ailleurs, toute utilisation ou reproduction intégrale ou partielle faite sans le consentement de OCI OUEST est illicite. Cette représentation ou reproduction par quel que procédé que soit constituerait une contrefaçon sanctionnée par les dispositions du Code de propriété intellectuelle et, de manière générale, une atteinte aux droits de OCI OUEST.

Ce document est diffusable sur demande d'une partie concernée. Cette PSSI pouvant évoluer, voir l'article « Évolution de la PSSI ». La partie prenante pourra demander à échéance régulière toute nouvelle version.

Contrôle d'application de la PSSI

L'ensemble des mesures évoquées dans la PSSI ainsi que dans toutes ses déclinaisons font l'objet de contrôles afin de s'assurer de l'applicabilité des mesures de sécurité. L'ensemble des contrôles sont dictés par un comité de sécurité ou du responsable de la sécurité de l'information (RSSI), et rendent compte à la direction à travers une revue de direction annuelle.

Les moyens de contrôle sont les suivants :

- Audit interne : Permettant de contrôler l'ensemble des mesures afin de valider ou exposer tout éventuelle non-conformité pour remédiation et correction de la cause.

- Audit externe : Réalisés par des prestataires externes afin de contrôler le niveau de conformité tant sur la PSSI que sur les différents référentiels associés.

- Revue de direction : Extraction des KPI ainsi que des résultats des différents audits afin de garantir la conformité du système d'information (SI) à la présente PSSI et aux référentiels associés.

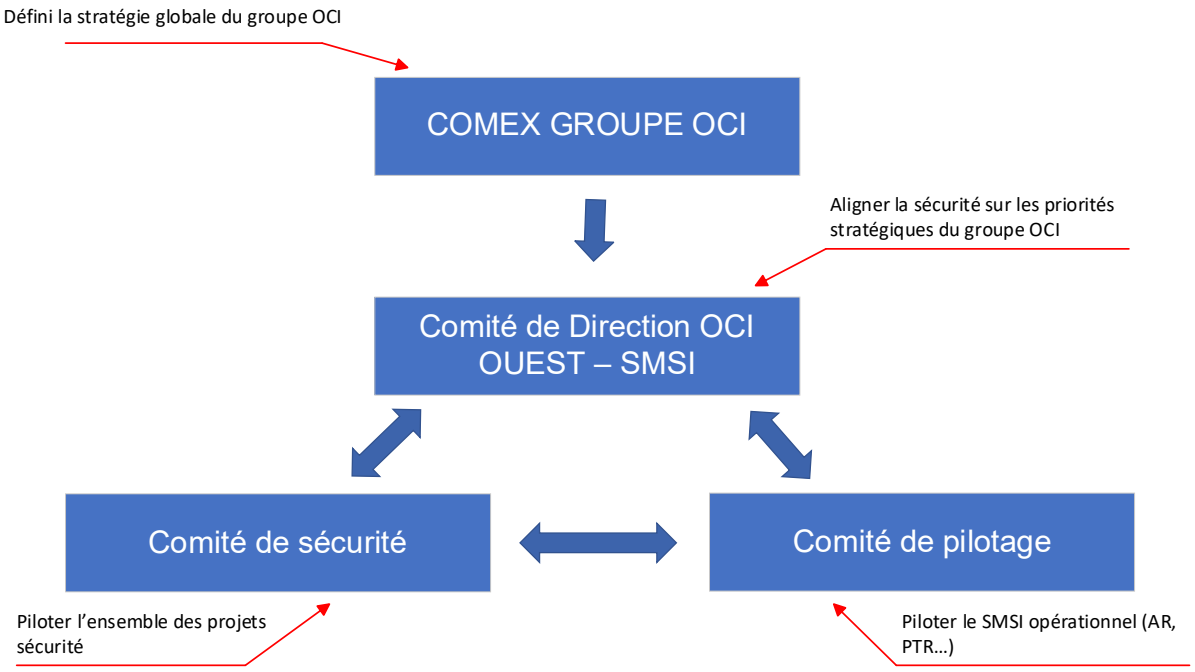
Principes organisationnels

1. Gouvernance du SMSI

Généralité

La direction générale soutient la présente politique de sécurité du système d'information (PSSI) sur son application au sein de OCI OUEST tout en portant les engagements en termes de sécurité. Elle soutient également les actions et les directives à mettre en œuvre pour protéger le patrimoine informationnel de l'entreprise.

Pour y parvenir, OCI OUEST a mis en place la gouvernance suivante :



Cycle de la gouvernance

Comité	Rôle	Cycle
Revue de direction du SMSI	Rend compte à la direction de l'état de santé du SMSI. Alignement de la sécurité sur les priorités stratégiques de OCI	Annuelle

	OUEST.	
Comité de sécurité	Suivi et pilotage de l'ensemble des projets visant à maintenir le niveau de sécurité exigé.	Trimestriel
Comité de pilotage	Suivi et pilotage de l'ensemble des projets visant à maintenir le niveau de conformité exigé.	Trimestriel

Acteurs de la sécurité

Un ensemble d'acteurs interviennent au cours de ces comités afin de répondre et d'effectuer le suivi des exigences de sécurités exigées par la direction.

- Un **Responsable de la Sécurité du Système d'Information (RSSI**) est nommé pour garantir les choix et décisions autour de la sécurité technique et humaine sur le SI.
- Un **Responsable du Système d'Information (RSI)** est nommé afin de garantir le développement, le pilotage projet et le maintien en conditions opérationnelles de l'infrastructure interne avec son équipe technique.
- Un **Responsable du SMSI (RSMSI)** est nommé afin de faciliter les interactions entre les différents comités.
- Un **représentant de l'équipe cybersécurité** est nommé afin d'apporter son expertise, apporter une veille cyber et expose les différents éléments de mesures (**KPI**).
- Un **juriste** participe aux échanges afin de veiller au respect des différentes législations en vigueur.
- Un **délégué à la protection des données (DPO)** est sollicité afin de veiller au respect à la Réglementation Générale de la Protection des Données (RGPD).

2. Gestion des risques

2.1. Méthodologie EBIOS

Afin de protéger l'ensemble des actifs mis à disposition par OCI OUEST, un management par les risques numérique est en place.
Cette gestion des risques est suivie par le **comité de sécurité** et repose sur la méthodologie **EBIOS RM** promue par **l'ANSSI.**

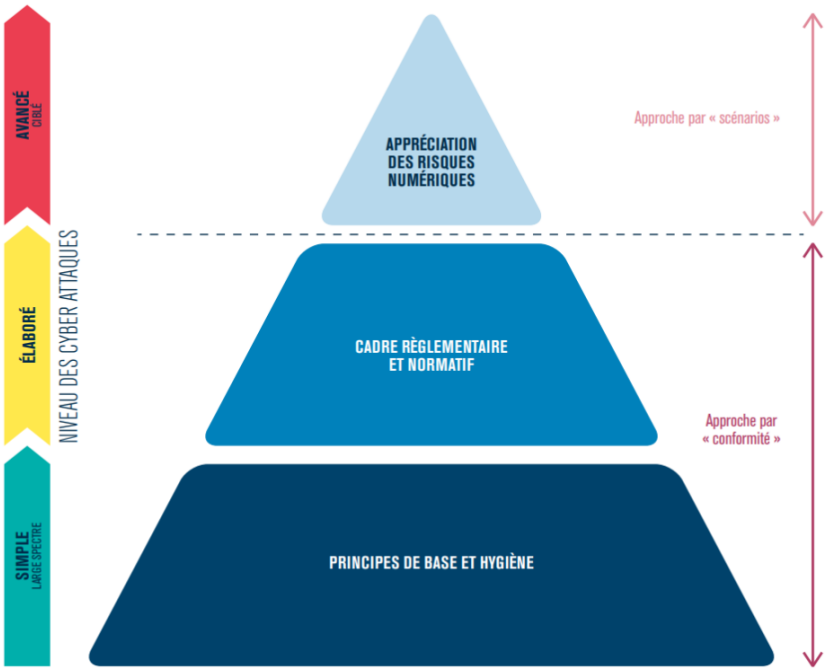


Figure 1: Pyramide du management du risque numérique - ANSSI

L'approche par « **conformité** » est constituée des principes de base ainsi que des cadres réglementaires et normatifs choisis par l'entreprise permettant de répondre au premier niveau.
L'approche par « **scénarios** » permet de répondre au plus haut niveau de cyberattaque. L'ensemble est ainsi représenté sous forme d'une pyramide de management du risque numérique.

2.2. Cycle de vie de l'analyse de risque

Le management par les risques numériques est effectué à travers cinq ateliers itératifs à réaliser de façon cyclique. L'objet de l'étude fait la distinction suivante :
Cycle stratégique [Tous les 3 ans] : Permets une approche par la conformité, mais également par scénario dans le but de couvrir les trois niveaux des cyberattaques.
Cycle opérationnel [Chaque changement majeur du SI ou à minima tous les ans] : Cycle afin de réaliser une approche par scénario dans le but de couvrir le plus haut niveau de cyberattaque.

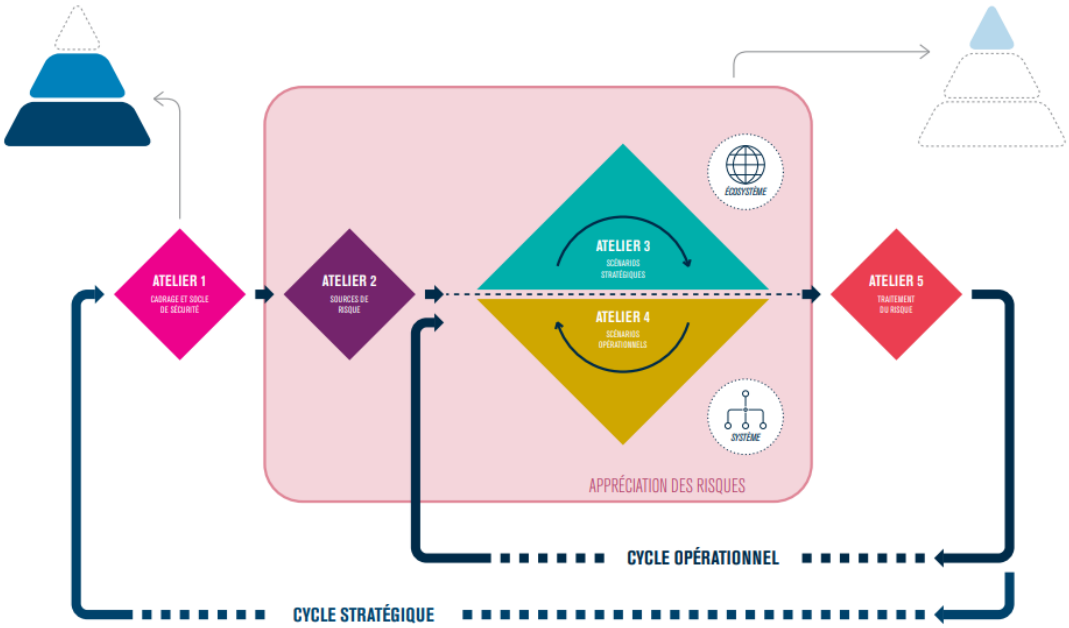


Figure 2 : Une démarche itérative en 5 ateliers – ANSSI

2.3. Sécurité dans les projets

Chaque projet interne visant à modifier le système d'information suit la conduite de projet suivante :

<u>Phase préparatoire :</u>

- Assurer la cohérence des enjeux et **besoins de sécurité du projet**
- Mise en place d'une **appréciation des risques**
- **Identifier les acteurs** clés nécessaires
- Validation du **scénario d'intégration et tests fonctionnels.**

<u>Phase de build :</u>

- Mise en place.
- **Validation** de la phase de build.
- Mise en place et **modification de la documentation nécessaire.**
- **Ajouts de KPI** ou de mécanismes de détection auprès du SOC.

<u>Phase de run :</u>

- Mise en place d'un **retour d'expérience projet (REX).**
- **Intégration** des nouvelles KPI lors des comités de sécurité.

3. Protection des informations

Afin de garantir la protection des informations confiées à OCI OUEST, l'ensemble des mesures suivantes sont en place :

- **Cartographie de l'information :** Ensemble de processus et de procédures permettant d'identifier et classifier l'information afin d'en déterminer la sécurité souhaitée en cohérence avec les différentes législations, normes, et exigences de la direction.
- **Contrôles d'accès :** Ensemble de processus et procédures visant à maîtriser le cycle d'accès (attribution, maintien, désaffectation) aux données.
- **Sensibilisations et formations des utilisateurs :** Chaque collaborateur est sensibilisé et formé en cohérence avec ses fonctions et périmètre (sensibilisation, RGPD, formation technique, sensibilisations aux normes 27001 et HDS[1]).
- **Suivi et audit :** Réalisation d'audit technique et de connaissance afin de s'assurer du respect des règles de sécurité.
- **Gestion des risques :** Afin de garantir le niveau de risque souhaité en cohérence avec le besoin de sécurité des données.

4. Échelle et critères de détermination des besoins de la sécurité

Afin de garantir un niveau de sécurité adapté à l'ensemble des actifs, OCI OUEST utilise le critère de classification nommée « **Critère DICT** » :

- **Disponibilité** : Besoin de disponibilité de l'actif en cohérence avec les législations, normes et volontés des parties prenantes.
- **Intégrité** : Besoin d'intégrité de l'actif en cohérence avec les législations, normes et volontés des parties prenantes.
- **Confidentialité** : Besoin de confidentialité de l'actif en cohérence avec les législations, normes et volontés des parties prenantes.
- **Traçabilité** : Besoin de traçabilité de l'actif en cohérence avec les législations, normes et volontés des parties prenantes.

La classification de chaque actif au critère DICT est défini par le **RSI**. Ce critère est **validé par le RSSI** avec **l'appui du service juridique** et **DPO**.

5. Gestion des accès

Afin de protéger les données en cohérence et garantir un niveau d'accès adéquat à la mission des collaborateurs et prestataires tiers, l'ensemble des mesures suivantes sont en place :

- **Principe du moindre privilège :** L'actif (donnée ou outil) n'est accessible que pour les besoins de la mission de la partie concernée et l'attribution des droits est effectuée en cohérence avec la matrice établie.
- **Traçabilité :** Utilisation d'un compte nominatif et/ou moyen de traçabilité pour avoir la capacité d'identifier toute personne accédant ou effectuant une manipulation de la donnée.
- **Utilisation du MFA :** La mise en place du MFA est obligatoire.
- **Usage du SSO :** Utilisation d'un dispositif permettant l'utilisation du compte AD comme moyen d'authentification.
- **Mots de passe complexes et politique de sécurité associée.**

La mise en place des accès est sous la **responsabilité du RSI**. La procédure et les règles sont sous la **responsabilité du RSSI**

Principe de mise en œuvre

1. Aspects humains

1.1. Clause de confidentialité

La sécurité de l'information concerne l'ensemble des collaborateurs de OCI OUEST. De ce fait, chaque collaborateur est contraint de signer une clause de confidentialité en sus de son contrat de travail, qui lui est remis au travers d'un lien de signature électronique en même temps que son contrat de travail lors de l'embauche.

1.2. Charte informatique

Une charte informatique définissant l'ensemble des règles et des bonnes pratiques d'utilisation des ressources informatiques de OCI OUEST est fournie lors de l'embauche au travers du livret d'accueil et doit être connue de l'ensemble des collaborateurs.

1.3. Charte administrateur

Une charte d'administrateur défini l'ensemble des règles et des bonnes pratiques d'administration des ressources informatiques.

1.4. Sélection du personnel qualifié

Afin de répondre aux besoins des parties prenantes, chaque offre d'emploi précise l'ensemble des qualités à la fois techniques et humaines nécessaires pour le poste.

La participation du responsable du service demandeur de la ressource humaine participe au processus de recrutement afin de valider les qualités recherchées.

2. Principes généraux d'habilitation

Chaque nouveau collaborateur se voit attribuer les accès physiques ainsi que logiques nécessaires à ses fonctions. L'ensemble des accès sont nominatifs et tracés sur une durée déterminée afin d'apporter des éléments de réponses en cas d'incident de sécurité.

Une politique spécifique nommée « **Politique de gestion des accès SI**» détaille l'ensemble des mesures de gestion des accès en vigueur. Cette politique est classifiée interne et n'est, comme toutes les autres politiques, pas publique.

3. Redondance des compétences

Chaque manager opérationnel a la charge du plan de formation et du plan de carrière de ses collaborateurs. Une révision des compétences s'effectue chaque année et permet de s'assurer d'avoir une disponibilité accrue des compétences et d'orienter les besoins en formation.

4. Planification de la continuité des activités

4.1. Plan de continuité de l'activité

Afin d'assurer la continuité des activités, un plan de continuité est documenté, révisé chaque année avec le suivi du comité de sécurité.

Le **plan de continuité d'activité (PCA)** contient :

- L'analyse de l'impact potentiel
- Les risques & menaces potentiels
- L'ensemble des mesures de continuité actuellement prévues et déployées
- La stratégie de continuité de l'activité
- Les processus et procédures associées
- Les conditions de maintiens des activités et de retour à la normale

4.2. Plan de reprise d'activité

Afin d'assurer la reprise des activités, un plan de reprise est documenté, révisé chaque année par le comité de sécurité.

Le **plan de reprise d'activité (PRA)** contient :

- L'analyse de l'impact potentiel
- Les risques & menaces potentiels
- L'ensemble des mesures de reprise actuellement prévues et déployées
- La stratégie de reprise de l'activité
- Les processus et procédures associées
- Les conditions de lancement du PRA et de retour à la normale

5. Gestion des incidents

5.1. Caractéristique d'un incident

Un incident de sécurité correspond à tout événement avéré ou suspecté ayant un impact négatif sur la sécurité des systèmes d'informations. Cela inclut, sans s'y limiter, les atteintes à la disponibilité, à l'intégrité, à la confidentialité ou à la traçabilité des données ou des services numériques.

Exemples d'incidents :

- Pannes ou anomalies de fonctionnement matérielles ;
- Pannes ou anomalies de fonctionnement des logiciels et applicatifs ;
- Production de résultats manquants, incomplets ou anormaux ;
- Problématique à la suite de données en entrées absentes, incomplètes ou anormales ;
- Accès non conforme à ce qui est attendu ;
- …

5.2. Dispositifs de détection et d'alerte des incidents

Afin de détecter tout incident, l'ensemble des dispositifs suivants sont en place :

- Antivirus Next-Gen couplé à un dispositif de type EDR monitorés par le service SOC interne ;
- Supervision du SI (équipements, réseau, serveurs, applicatifs,) gérés par le service Informatique Interne ;
- Centralisation des logs
- Gestion des vulnérabilités prises en charge par le service informatique interne et Hébergement avec le soutien du comité de sécurité ;
- Ensemble de contrôles techniques et organisationnels permettant la surveillance du SMSI ;
- Obligation de toute remontée d'éventuel incident observé immédiatement.
- Audit technique et organisationnel.

5.3. Déclaration et gestion des incidents

Tout incident fait l'objet d'un ticket de type « incident » permettant la déclaration et le suivi du traitement. En cas d'incident impactant plus de la moitié du personnel, cet incident est considéré comme majeur.

Tout incident majeur peut mener à une ouverture de gestion de crise et sa résolution donne lieu à un retour d'expérience et d'un plan d'action **suivi par le comité de sécurité.**

5.4. Déclaration et gestion d'un problème

Une répétition d'un incident de sécurité au sens DICT (à partir de 3 itérations) donne lieu à la création d'un incident de type « problème ». Ce type d'incident permet de regrouper les parties prenantes afin d'identifier la faille dans le processus et la méthodologie afin d'y remédier pour empêcher l'apparition nouvelle de l'incident.

6. Sensibilisation et formation

6.1. Sensibilisation et formation à la sécurité

L'ensemble des employés sont sensibilisés dès leur arrivée avec la présentation de l'ensemble du corpus documentaire jugé nécessaire vis-à-vis de ses fonctions et de la charte informatique au travers d'un guide d'accueil. Il existe un guide d'accueil commun à tous les salariés, ainsi que des guides spécifiques par service pour les services concernés.

Tout au long du parcours de l'employé, ce dernier bénéficie de campagne de sensibilisation spécifique à ses fonctions sur les sujets suivants :

- Processus internes
- Sécurité numérique
- RGPD
- Respect du code de la propriété intellectuelle
- ISO 27001 & HDS[2]
- ….

6.2. Communication sur la SSI

Tout au long de l'année, OCI OUEST effectue pour l'ensemble de ses collaborateurs différentes communications (enjeux internes, mesures de sécurité, veilles, etc.) à travers les canaux internes (mails, intranet).
En cas de suspicion d'un incident de sécurité, voici la liste des différents canaux en fonction du contexte :

Contexte	Contact – OCI OUEST
Atteinte à la donnée personnelle	DPO + RSSI + Équipe technique informatique interne + Juriste + RSI + RSMSI
Incident de sécurité	Équipe cybersécurité + DPO + RSSI + Équipe technique interne + Juriste +RSI + RSMSI

7. Exploitation

7.1. Règle d'utilisation du SI

La présence d'une charte informatique et charte administrateur rappelle les règles et conditions d'utilisation du SI. Chaque collaborateur en prend connaissance lors de son arrivée et chaque modification donne lieu à une communication interne.

7.2. Documentation des procédures et règles d'exploitation

Toutes activités de MCO font l'objet d'une documentation centralisée, historisée et sous accès restreint aux services concernés internes.
Cette documentation pourra, selon les besoins, donner lieu à plusieurs documents, chacun étant destiné à une catégorie d'acteurs concernés en fonction de son rôle, de ses responsabilités et de son besoin d'en connaître.
Cette documentation est transmise sur demande motivée du client.

7.3. Conditions applicables à l'infogérance OCI OUEST

Afin de faciliter l'infogérance pour nos clients, OCI OUEST met à disposition :

- Un outil de télémaintenance centralisé permettant de se connecter sur l'ensemble des ressources chez les clients avec leur approbation, à destination de nos forces techniques ;
- Un portail Client à destination de l'ensemble des clients afin qu'ils puissent suivre leurs contrats, leurs tickets, les RDV tels que les régies et sur demande l'accès au dossier Client comportant les informations sensibles du DAT (Dossier d'Architecture Technique) ;
- Du matériel interne sécurisé pour le personnel (smartphone, PC portable) ;
- Des plateformes d'infogérance (Cloud, supervision, patch management, etc) soumis à cette PSSI et à des PSSI complémentaires selon le cas.

Chaque composante des offres commerciales de OCI OUEST repose sur le standard du « **Security by Design** », qui sont décrits lorsqu'applicables dans contrats ou nos CGV.

8. Préventions des vulnérabilités

Afin de se prémunir des vulnérabilités du système qui pourrait être pris pour cible, le SI suit les principes suivants :

- Architecture respectant le principe de la défense en profondeur ;
- Prise en compte des best practices préconisées par les différents éditeurs ;
- Processus de Patch Management et de Security Patch Management. ;
- Obligation d'une solution MFA pour l'accès à l'ensemble des ressources depuis l'externe mais aussi pour l'accès aux serveurs internes ;
- Priorisation des projets en fonction des risques identifiés ;
- Audit interne (vulnérabilité, pénétration externe, audit de configuration …) ;
- Mise en place d'outils de prévention (antivirus, EDR, scanner de vulnérabilités, filtrage mails, …) ;
- Sensibilisation du personnel ;
- Politique de gestion des accès ;
- Audit d'accès ;
- Analyse quotidienne des CVE par « une sentinelle » ;

Aspects physiques et environnementaux

1. Prévention des menaces environnementale

Afin de se prémunir de toute menace physique ou environnementale, les systèmes sensibles ou vitaux sont hébergés dans des datacenters.

Les datacenters :

- Répondent à la classification de tiers 3+ ;
- Sont certifiés ISO 27001 et HDS ;
- Son équipés de dispositifs anti-intrusion ;
- Sont protégés électriquement (redondance, onduleurs, …) ;
- Sont équipés de systèmes de protections environnementales (filtrage de la poussière, système anti-incendie, …)

2. Mesures de sécurité physique

2.1. Découpage de l'infrastructure en zones de sécurité

Les locaux exploités par OCI OUEST respectent le principe de défense en profondeur ainsi, chaque local est protégé par un premier niveau d'accès par code d'accès
Un second niveau d'accréditation permet l'accès aux infrastructures du SI (Baie de brassage, switch, …) dans les différentes agences.
Un dernier niveau d'accréditation permet l'accès aux infrastructures physique au datacenter.
Ces accès sont accordés en cohérence avec les missions du collaborateur et sont tracés et audités.
Les locaux disposent de mesures anti-intrusion (détecteurs de présence, caméra …).

2.2. Protection contre les accidents et pannes physique.

Afin de se prémunir d'accidents et de pannes, les équipements physiques sont redondés ou, dans le cas contraire, identifiés et disposent de mesures spécifiques et documentés notamment dans le cadre du PCA / PRA.
Tout équipement de protection environnemental est contrôlé conformément aux réglementations en vigueur.

Principes techniques

1. Identification / authentification

1.1. Utilisation du SSO

Chaque outil pouvant utiliser les technologies d'authentification unique (Kerberos, SAML, OAuth, OpenID, ...) doit être utilisé afin de centraliser et simplifier la gestion des accès.

1.2. Authentification MFA

L'accès initial au système d'information passe par une double authentification (Token MFA). Seule exception faite pour les réseaux filaires des agences OCI, qui est justifiée par des moyens d'authentification d'accès aux bâtiments (radius).

1.3. Séparation des comptes d'utilisation et d'administration

Afin de réduire le risque de compromission, toute personne administrant le Système d'information utilise un compte d'administration nominatif séparé de son compte utilisateur. Ce compte comporte également les mesures de sécurité suivantes :

- Journalisation des actions,
- Authentification via MFA sur chaque serveur,
- Politique de renouvellement de mots de passe.

1.4. Stratégie de mot de passe

L'ensemble des identifiants internes suivent les restrictions préconisées par l'ANSSI, à savoir :

Utilisateurs :

- Renouvellement annuel des mots de passe ;
- Complexité de mot de passes suivant : 14 Caractères minimum, dont au moins une majuscule, au moins un caractère spécial et au moins un caractère alphanumérique.
- Le mot de passe doit être différent des 5 derniers mots de passe.

Administrateurs :

Des règles spécifiques et confidentielles sont appliquées aux mots de passe des comptes d'administration et sont documentés et suivi par des moyens de contrôles.

1.5. Utilisation d'un gestionnaire de mot de passe

Chaque collaborateur identifié comme ayant besoin d'un gestionnaire de mot de passe par le RSSI dispose d'un gestionnaire de mot de passe approuvé afin de stocker de façon sécurisée l'ensemble de ses mots de passe.

1.6. Délivrance et recouvrement des moyens d'authentifications

Chaque envoi d'identifiant se fait exclusivement à l'aide d'un outil de partage sécurisé.
Chaque distribution d'accès se fait à travers deux canaux de communication distincts :

- Communication par mail contenant le lien sécurisé avec délai d'expiration.
- Envoi à travers un canal établi en amont (teams / vocal / SMS / …) le mot de passe permettant d'ouvrir le lien sécurisé

Lors de chaque modification à la suite de la perte d'un mot de passe, il est demandé de changer son mot de passe après une première connexion.

Tout départ d'un collaborateur se solde par une désactivation de son compte utilisateur et des comptes liés hors SSO sur des plateformes tierces du SI le jour J (qui sont donc documentées et tracées dès la phase de création) pendant 1 mois puis supprimé de manière automatique. L'ensemble des mécanismes sont détaillés dans la politique de flux RH, et informatique interne.

2. Sauvegarde

L'ensemble des données hébergées par le SI, en central dans les Datacenters ainsi qu'en agence, sont sauvegardées selon les bonnes pratiques de sauvegarde (3-2-1).

L'ensemble des mesures techniques ne sont pas documentées dans cette version publique de notre PSSI.

3. Contrôle d'accès logique

3.1. Dispositifs et procédures de protection contre les intrusions

Afin de protéger l'ensemble des communications du système d'information, ce dernier est protégé par l'ensemble de dispositifs suivants :

- Authentification extérieure à l'aide de CITRIX ou PARALLELS.
- Géo restriction.
- Filtrage Web + UTM.
- Segmentation réseau.

3.2. Cloisonnement des réseaux et maîtrise des flux

Le cloisonnement des réseaux a pour objectif :

- De faciliter le contrôle d'accès ;
- De mieux se protéger contre les intrusions (défense en profondeur) ;
- D'empêcher la fuite d'information.

Le cloisonnement respecte le principe du moindre privilège et nous distinguons quatre familles de cloisonnement elles-mêmes subdivisées en fonction des besoins.

Accessible depuis l'extérieur : Ensemble de zones démilitarisées (DMZ) pour tout actif accessible depuis l'extérieur (Site Web par exemple).

Réseau interne utilisateur : Réseau sécurisé accessible pour l'ensemble des collaborateurs afin d'accéder aux différents actifs du groupe.

Réseau d'administration technique : Réseau uniquement accessible par les comptes administrateurs pour la mise en place et administration des actifs du SI (Serveurs, switch,).

Réseau invité : Réseau mis à disposition pour les parties prenantes externes présentes dans les locaux (Wifi-invité).

4. Modalités d'utilisation sécurisée des réseaux de télécommunication de l'organisme

L'accès initial à chaque réseau se fait à travers un compte nominatif. Le réseau interne ne peut être accessible en externe qu'à l'aide d'une connexion sécurisée.
L'ensemble des cloisonnements réseaux est répertorié dans l'outil de cartographie de l'information. Les accès au management des actifs sont inventoriés et managés par le responsable de l'actif.

5. Journalisation

5.1. Moyens de journalisation communs

Le RSSI détermine pour chaque élément du SI les rétentions jugées adéquates afin d'avoir la capacité de répondre à toute investigation en cas d'incident.
Un niveau d'accréditation est nécessaire pour accéder à ces journaux et ces derniers sont sauvegardés, la sauvegarde faisant elle-même partie de l'analyse de la rétention souhaitée.

5.2. Enregistrement des opérations

Du fait des technologies actuellement déployées et des journalisations activées sur l'ensemble du SI, l'ensemble des opérations sont enregistrées à des fins de preuve.

5.3. Alertes de sécurité

Pour toute alerte de sécurité générée par un outil de détection, l'équipe SOC dispose de processus et procédures afin de qualifier et traiter les alertes de sécurité.

En cas d'alerte avérée et de leur classification définie dans la procédure de gestion des incidents, un ensemble de mesures sont appliquées allant jusqu'à l'ouverture d'une cellule de crise.

Pour chaque alerte avérée, le groupe effectue un retour d'expérience à la fin de l'incident afin d'améliorer les processus et procédures existants. Les différents journaux en place sont consultés à des fins de compréhension lors de l'analyse et réexploités lors des RETEX.

5.4. Constitution de preuves

En cas d'incident, la constitution d'éléments de preuves informatiques se fait conjointement avec le service juridique interne afin de garantir le respect de la législation en vigueur.

Une procédure de réquisition judiciaire est également disponible et mise à jour par le service juridique.

6. Infrastructures de gestion des clés cryptographiques

6.1. Généralité

Pour répondre à différents besoins de sécurité de OCI OUEST, les communications sont chiffrées à l'aide d'algorithme cryptographique et de certificats TLS.

6.2. Algorithmes cryptographiques

Afin de se prémunir d'algorithmes désuets, OCI OUEST utilise des algorithmes jugés robustes lors de l'établissement des éléments du SI.
Le comité de sécurité assurant la veille cyber met à jour la liste des algorithmes jugés robustes et assure tout suivi de changement d'algorithme.

6.3. Gestion des certificats

Un processus de gestion des certificats et des procédures techniques est en place afin de maintenir l'ensemble des certificats utilisés par le SI et assurer leurs renouvellements et leur sécurité.

6.4. Protection des clés

Toute clé utilisée pour chiffrer les moyens de communication est centralisée dans un gestionnaire de mots de passe. L'accessibilité de ces clés se fait uniquement à travers un réseau approuvé et avec une accréditation restreinte aux seules personnes dont la mission est de maintenir les moyens chiffrements.

7. Signaux compromettants

7.1. Généralité

Tout matériel ou système qui traite des informations sous forme électrique est le siège de perturbations électromagnétiques. Ces perturbations, provoquées par le changement d'état des circuits qui composent le matériel considéré, sont qualifiées de signaux parasites. Certains de ces signaux sont représentatifs des informations traitées. Leur interception et leur traitement permettent de reconstituer ces informations. Ces signaux sont, de ce fait, dénommés "signaux parasites compromettants".

7.2. Cages de Faraday

L'ensemble des datacenters qui hébergent les éléments du SI jugé vitaux pour effectuer les missions de OCI OUEST sont protégés par des cages de Faraday.