

Abidjan, le 22 JAN. 2026

NOTE DE SERVICE
DG/SSI/ N°001/ 2026

Objet : ENGAGEMENT DE LA DIRECTION GENERALE EN MATIÈRE DE POLITIQUE DE SÉCURITÉ

Mesdames et messieurs,

En vue de faire face à des risques de plus en plus importants, CI-ENERGIES renforce la sécurité de son Système Informatique en s'engageant dans la mise en œuvre d'un Système de Management de la Sécurité de l'Information. Ce système a pour objectif de maintenir un niveau de sécurité acceptable sur tous les actifs de CI-ENERGIES ; ce qui contribuera à renforcer la confiance de nos partenaires techniques et financiers.

La Politique de Sécurité de l'Information (PSI) qui émane de cette démarche sécurité est déclinée en règles organisationnelles et techniques pour la protection de notre Système Informatique et de nos actifs. Elle s'applique à toutes les directions, ainsi qu'à tous les départements et services qui utilisent les ressources de l'entreprise. Nos partenaires et nos sous-traitants sont également tenus de s'y conformer.

Ainsi, la PSI de CI-ENERGIES s'appuie sur (5) cinq objectifs clés :

- Garantir la sécurité des données sensibles de l'entreprise et celles à caractère personnel de nos clients et de nos collaborateurs ;
- Garantir la gestion des risques et assurer la protection contre les menaces et cyberattaques ;
- Maîtriser les risques de la sécurité de l'information liés aux fournisseurs et partenaires ;
- Assurer la continuité de nos activités et services essentiels ;
- Assurer la conformité aux exigences contractuelles, légales et réglementaires.

L'appropriation et le respect des exigences de cette politique constituent un enjeu crucial pour le bon développement de notre entreprise.

Aussi, en ma qualité de Premier Manager de l'entreprise, je m'engage avec l'ensemble du Comité de Direction à veiller au respect scrupuleux des dispositions prévues dans cette politique en vue de la mise en œuvre efficace et de l'amélioration continue du Système de Management de la Sécurité de l'Information. Nous nous engageons également au respect des obligations légales et réglementaires ainsi qu'à satisfaire l'ensemble des exigences applicables.

.../...

A notre suite, tout le personnel de CI-ENERGIES est engagé à la mise en œuvre de notre Politique de Sécurité de l'Information dont l'implémentation, la supervision, et le suivi quotidien sont assurés au Responsable Sécurité des Systèmes de l'Information (RSSI), qui me rendra régulièrement compte.

Enfin, j'invite tout le personnel à prendre connaissance de la politique de sécurité du Système d'Information de notre entreprise. Cela permettra à chacun de connaître et d'appliquer les principes et les règles sur la gestion de la sécurité de nos systèmes d'information.

Car la sécurité, c'est l'affaire de tous. 

Le Directeur Général



Noumory SIDIBE

Destinataires

- DG
- SG
- DCSA
- DCEP
- DCET
- DCAF

Tableaux d’Affichage

- DG
- Centre médical (1)
- Atelier central (1)
- CRT
- Centrale de Soubré
- Centrale Gribo-Popoli
- Centrale de Boundiali

Copie

- Secrétariats (20)

Politique de Sécurité de l'Information

Juillet 2025

Document	<i>Politique de sécurité de l'Information</i>		
Version	0.1		
Rédacteur	Relecture	Validation	Information
RSSI			Personnel

CI-ENERGIES

Chief de service sécurité
des systèmes d'information

[Signature]

YOUSSEUF SOUMAHORO

CI-ENERGIES

Directeur des Systèmes
d'information

[Signature]

OUSSENI ROMBA



Table des matières

ENGAGEMENT DE LA DIRECTION GENERALE	5
TERMINOLOGIE	7
1. INTRODUCTION	10
1.1. Objet de la présente politique	10
1.2. Périmètre d'application de la PSI	10
1.3. Obligations et normes applicables	11
1.3.1. Code de conduite	11
1.3.2. Normes et référentiels	11
1.4. Cadre légal et réglementaire	12
1.4.1. Au niveau national	12
1.4.2. Au niveau international	12
2. RESPONSABILITÉS ET GOUVERNANCE.....	13
2.1. Synthèse de l'organisation	13
2.2. Comité Exécutif de Sécurité SI	13
2.3. Le Comité de Sécurité du SI	14
2.4. Le Comité Opérationnel de sécurité du SI	14
2.5. Le RSSI de CI-ENERGIES :	15
2.6. Correspondant Sécurité SI.....	15
2.7. Les experts en sécurité de l'information.....	16
2.8. Tous les Employés :	16
2.9. Tableaux de bord.....	16
3. LES PRINCIPES DIRECTEURS	17
3.1. Approche holistique	17
3.2. Responsabilisation	17
3.3. Proportionnalité.....	18
3.4. Proactivité	18
3.5. Visibilité	19
3.6. Amélioration continue	19
3.7. Principe de cohérence.....	19
3.8. Principe d'efficacité	19

3.9.	Principe de pérennité	20
3.10.	Principes de conformité	20
3.11.	Principe d'exception documenté	20
4.	PRINCIPES DE SECURITE	21
4.1.	Les principes de mise en œuvre.....	21
4.1.1.	La gestion des risques SSI	21
4.1.2.	La sécurité et le cycle de vie du logiciel	21
4.1.3.	Conformité et audits	22
4.1.4.	Les aspects humains	22
4.1.5.	La gestion des actifs	22
4.1.6.	La planification de la continuité des activités	22
4.1.7.	La gestion des incidents.....	23
4.1.8.	La sensibilisation et la formation	23
4.1.9.	L'exploitation.....	23
4.1.10.	Infogérance	23
4.1.11.	Les aspects physiques.....	24
4.2.	Les principes techniques	24
4.2.1.	Gestion des identités et des accès.....	24
4.2.2.	Sécurité des applications.....	24
4.2.3.	La sécurité des réseaux.....	25
4.2.4.	La sécurité des systèmes industriels.....	25
4.2.5.	L'administration des serveurs et des postes de travail	26
4.2.6.	La journalisation.....	26
4.2.7.	Les infrastructures de gestion des clés cryptographiques	26
4.2.8.	Cyber surveillance et signaux de compromission.....	27
4.2.9.	La sécurité physique.....	27
5.	LA MISE EN APPLICATION ET LE SUIVI DE LA POLITIQUE DE SECURITE	28
5.1.	Validation de la politique de sécurité	28
5.2.	Diffusion et classification de la politique de sécurité.....	28
5.3.	Evolution de la politique de sécurité	28
5.4.	Gestion des dérogations	28

Abidjan, le 22 JAN. 2026

NOTE DE SERVICE
DG/SSI/ N°001/ 2026

Objet : ENGAGEMENT DE LA DIRECTION GENERALE EN MATIÈRE DE POLITIQUE DE SÉCURITÉ

Mesdames et messieurs,

En vue de faire face à des risques de plus en plus importants, CI-ENERGIES renforce la sécurité de son Système Informatique en s'engageant dans la mise en œuvre d'un Système de Management de la Sécurité de l'Information. Ce système a pour objectif de maintenir un niveau de sécurité acceptable sur tous les actifs de CI-ENERGIES ; ce qui contribuera à renforcer la confiance de nos partenaires techniques et financiers.

La Politique de Sécurité de l'Information (PSI) qui émane de cette démarche sécurité est déclinée en règles organisationnelles et techniques pour la protection de notre Système Informatique et de nos actifs. Elle s'applique à toutes les directions, ainsi qu'à tous les départements et services qui utilisent les ressources de l'entreprise. Nos partenaires et nos sous-traitants sont également tenus de s'y conformer.

Ainsi, la PSI de CI-ENERGIES s'appuie sur (5) cinq objectifs clés :

- Garantir la sécurité des données sensibles de l'entreprise et celles à caractère personnel de nos clients et de nos collaborateurs ;
- Garantir la gestion des risques et assurer la protection contre les menaces et cyberattaques ;
- Maîtriser les risques de la sécurité de l'information liés aux fournisseurs et partenaires ;
- Assurer la continuité de nos activités et services essentiels ;
- Assurer la conformité aux exigences contractuelles, légales et réglementaires.

L'appropriation et le respect des exigences de cette politique constituent un enjeu crucial pour le bon développement de notre entreprise.

Aussi, en ma qualité de Premier Manager de l'entreprise, je m'engage avec l'ensemble du Comité de Direction à veiller au respect scrupuleux des dispositions prévues dans cette politique en vue de la mise en œuvre efficace et de l'amélioration continue du Système de Management de la Sécurité de l'Information. Nous nous engageons également au respect des obligations légales et réglementaires ainsi qu'à satisfaire l'ensemble des exigences applicables.

.../...

A notre suite, tout le personnel de CI-ENERGIES est engagé à la mise en œuvre de notre Politique de Sécurité de l'Information dont l'implémentation, la supervision, et le suivi quotidien sont assurés au Responsable Sécurité des Systèmes de l'Information (RSSI), qui me rendra régulièrement compte.

Enfin, j'invite tout le personnel à prendre connaissance de la politique de sécurité du Système d'Information de notre entreprise. Cela permettra à chacun de connaître et d'appliquer les principes et les règles sur la gestion de la sécurité de nos systèmes d'information.

Car la sécurité, c'est l'affaire de tous. 

Le Directeur Général



Noumory SIDIRE

Destinataires

- DG
- SG
- DCSA
- DCEP
- DCET
- DCAI

Tableaux d’Affichage

- DG
- Centre médical (1)
- Atelier central (1)
- CRT
- Centrale de Soubré
- Centrale Gribo-Popoli
- Centrale de Boundiali

Copie

- Secrétariats (20)

TERMINOLOGIE

Authentification : processus employé pour faire la preuve de son identité en vue d'exercer ses droits sur un système.

Bien / Actif : tout élément représentant de la valeur pour l'organisme. On distingue les biens humains, des biens informationnels, matériels, logiciels ou logistiques.

Domaine d'activité : ensemble d'activités, de savoir-faire et des techniques associés à un métier.

Enjeu : ce que l'on peut gagner ou perdre dans une entreprise, un domaine d'activité ou un projet. L'enjeu peut être financier, commercial, organisationnel ou technique.

Entité : groupe d'individus partageant, sous la responsabilité d'un même manager, une mission commune et disposant d'une autonomie de décision.

Exigences de sécurité : expression de besoins de sécurité et de contrôles associés à une information ou à une ressource. Elles sont spécifiées en termes de : confidentialité, intégrité, disponibilité et contrôle d'accès.

- **Confidentialité** : propriété d'une information ou d'une ressource de n'être accessible (création, modification, diffusion, sauvegarde, archivage, destruction) qu'aux utilisateurs autorisés.
- **Intégrité** : propriété d'exactitude et de complétude des informations et des fonctions de l'information traitée. Celles-ci ne doivent pouvoir être modifiées que par un acte volontaire et légitime.
- **Disponibilité** : propriété d'accessibilité dans des conditions définies d'horaires, de délais et de performances des informations et des fonctions par les utilisateurs autorisés.
- **Contrôle d'accès** : capacité à restreindre l'accès à une information ou à une ressource aux utilisateurs légitimes par des contrôles appropriés exercés sur leurs droits.

Equipement réseaux et SI : tout élément ou sous-ensemble qui remplit une fonction particulière nécessaire au fonctionnement des Réseaux et SI. §

Identification : processus de déclinaison de son identité au moyen d'un code décrit dans un système d'annuaire donné.

Impact ou préjudice : conséquence sur l'entité de l'altération d'un bien.

Information : élément de connaissance susceptible d'être représenté sous une forme adaptée à une communication, un enregistrement ou un traitement.

Inventaire : description détaillée des biens (identification, propriétaire, localisation géographique, versions, raccordement au réseau, exigences de sécurité, etc...).

Manager : responsable d'une équipe ou d'un domaine d'activité.

Menace : cause potentielle d'incident qui exploite une vulnérabilité intrinsèque d'un bien. Elle peut être intentionnelle ou accidentelle. Une menace intentionnelle est réalisée par un agresseur qui a des motivations, elle nécessite des moyens (financiers et techniques) et du temps. Une menace peut également survenir à la suite d'une erreur, d'un phénomène naturel ou d'un accident.

Métier : domaine d'activité d'une entité.

Niveau des exigences de sécurité : formalisation selon une graduation de l'importance apportée à chacune des exigences.

Principe : expression de contraintes (lois, règlements, environnement technique) et d'orientations de sécurité pour l'élaboration d'une politique. Les principes doivent permettre l'élaboration de règles.

Profil : ensemble de droits qui définissent le comportement qu'un utilisateur peut exercer au sein d'une application.

Règle ou Règle de sécurité : exigence élémentaire de sécurité à appliquer à un sous-ensemble défini du système d'information, en vue de réduire la probabilité ou l'impact d'un événement redouté ou d'en prévenir le risque de survenance. §

Ressource d'information : élément du patrimoine de l'entité contribuant à la création, au traitement, au transport, au stockage, à l'archivage ou à la destruction de l'information.

Risque : combinaison de la probabilité d'un événement et de ses conséquences.

Sécurité : état de protection, face aux risques identifiés, qui résulte de l'ensemble de mesures générales et particulières prises pour satisfaire aux exigences de sécurité concernant l'information et les ressources associées.

Ces mesures peuvent se décliner en fonction du contexte (sécurité de l'information, sécurité des personnes, sécurité des biens physiques, ...)

Sensibilité : évaluation de l'impact sur l'entité, de la perte, du vol ou de l'altération d'une information.

Site : ensemble d'immeubles et installations construits sur un espace connexe contrôlé par CI-ENERGIES.

Sûreté des biens physiques : ensemble des mesures de protection contre les événements malveillants. Ces mesures portent notamment sur les contrôles d'accès physiques aux sites (protection périphérique), aux bâtiments (protection périmétrique), aux locaux et aux matériels (protection intérieure), en mode nominal, dégradé ou en crise.

SI : ensemble des ressources réseaux et informatiques destinées à élaborer, collecter, traiter, stocker, acheminer, présenter et détruire l'information.

Vulnérabilité : faille dans un bien/actif ou dans une mesure de sécurité qui peut être exploitée par une menace.

COBIT (Control Objectives for Information and Related Technology) : référentiel qui aide les entreprises à diriger et contrôler leurs systèmes d'information 8

1. INTRODUCTION

1.1. Objet de la présente politique

La politique de sécurité des systèmes d'information (PSI) de CI-ENERGIES est le document de référence pour la sécurité du SI de CI-ENERGIES.

C'est le document principal qui sera décliné en politiques thématiques et procédures décrivant les mesures de sécurité applicables au sein de CI-ENERGIES pour atteindre les objectifs de sécurité du SI.

La sécurité des informations se définit classiquement comme la maîtrise de la disponibilité, de l'intégrité et de la confidentialité de l'information. Elle se complète par le principe d'auditabilité qui répond aux besoins de traçabilité (piste d'audit, journaux d'activités, éléments de preuve, etc.).

Les objectifs de cette politique sont donc de garantir :

- La **confidentialité**, Propriété assurant qu'un système, une fonction ou une information n'est pas accessible ou communiqué d'une manière non autorisée.
- L'**intégrité** : Propriété assurant qu'un système, une fonction ou une information ne subit pas de modification d'une manière non autorisée.
- La **disponibilité** : Propriété assurant qu'un système, une fonction ou une information n'est pas rendu inaccessible d'une manière non autorisée ou accidentelle,
- L'**audibilité** : Capacité d'un système ou d'une fonction à fournir des éléments objectifs permettant à tout moment d'établir la conformité aux exigences, réglementaires ou légales.

1.2. Périmètre d'application de la PSI

Le périmètre de la PSI couvre l'ensemble des systèmes d'information de CI-ENERGIES et s'applique à tous ses actifs.

La PSI couvre l'ensemble des processus, des données et leur traitement (création, stockage, échange, etc.), que le format soit matériel ou immatériel (électronique, imprimé, oral, image, etc.) dans toute l'organisation.

Ainsi, elle s'applique :

- À l'ensemble du personnel permanent ou temporaire de l'entreprise, travaillant au sein de l'entreprise ou à distance ;
- À l'ensemble des partenaires de l'entreprise, qu'il s'agisse de personnes physiques ou morales (sous-traitants, prestataires de services, fournisseurs), ayant accès au système d'information de CI-ENERGIES ;

- À tous les matériels et logiciels permettant le traitement des données et/ou la réalisation des processus de production de CI-ENERGIES ;
- A tous les processus qu'ils soient de pilotage, métiers ou de support.

1.3. Obligations et normes applicables

1.3.1. Code de conduite

Tout utilisateur des systèmes d'information de CI-ENERGIES, quels que soient son statut et sa fonction, est un acteur de la sécurité de l'information. Il doit, à ce titre, respecter les règles et procédures en vigueur, conformément aux dispositions de la « Charte pour l'utilisation des systèmes d'information ».

En cas de violation des dispositions de la PSI, CI-ENERGIES procède à une évaluation de la portée des dommages subis ou des manquements occasionnés et, suivant leur gravité, décide des sanctions administratives et disciplinaires, sans préjudice d'éventuelles poursuites judiciaires.

1.3.2. Normes et référentiels

La démarche de CI-ENERGIES en matière de sécurité de l'information s'appuie sur un cadre de référence constitué d'une part, par le référentiel COBIT pour la gouvernance des systèmes d'information et, d'autre part, par la série des normes ci-après :

- ISO/IEC 27001 :2022 : Pour la gouvernance de la sécurité de l'information
- ISO/IEC 27002 :2022 : Reference pour les mesures de sécurité à mettre en œuvre pour le SI dans son ensemble
- ISO/IEC 27005 :2022 : Pour la Gestion des risques SI
- ISO/IEC 27019 :2024 et ISA/IEC 62443 : Références pour les mesures de sécurité permettant de contrôler et de surveiller la production, le transport, le stockage et la distribution de l'électricité, ainsi que pour le contrôle des processus support associés. A noter que cette norme est une adaptation de ISO27002 :2022 au secteur de l'électricité.
- ISO/IEC 62351 :2017 : référence pour la cybersécurité pour les systèmes de communication et de contrôle des réseaux électriques intelligents.

Ces choix permettent de définir un cadre de cohérence pour l'ensemble des acteurs : décideurs, métiers, techniciens, partenaires et prestataires. ✱

1.4. Cadre légal et réglementaire

1.4.1. Au niveau national

L'environnement juridique qui encadre la PSI est constitué des textes suivants :

- L'Ordonnance N°2024-958 Du 30 Octobre 2024 Portant Création, Attributions, Organisation et Fonctionnement de L'agence Nationale de la Sécurité des Systèmes d'information ;
- Le décret n° 2021-915 du 22 décembre 2021 a adopté la PSSI pour l'administration publique ivoirienne ;
- Le décret n° 2020-128 du 29 Janvier 2020 portant création, organisation et fonctionnement du centre de veille et de réponse aux incidents de sécurité informatique (CI-CERT) ;
- L'Ordonnance N° 2017-500 Du 02 Aout 2017 Relative aux Echanges Electroniques Entre les Usagers et les Autorités Administratives et entre les Autorités Administratives (Modifiée)
- La loi n° 2017-803 du 7 décembre 2017 d'orientation de la Société de l'information en Côte d'Ivoire ;
- Le décret n° 2016-851 du 19 octobre 2016 fixant les modalités de mise en œuvre de l'archivage électronique ;
- Le décret n° 2014-105 du 12 Mars 2014 portant définition des conditions de fourniture des prestations de cryptologie ;
- Le Décret n° 2014-106 du 12 Mars 2014 fixant les conditions d'établissement et de conservation de l'écrit et de la signature sous forme électronique ;
- La Loi n° 2013-450 du 19 juin 2013 relative à la protection des données à caractère personnel ;
- La Loi n° 2013-451 du 19 Juin 2013 relative à la lutte contre la cybercriminalité ;
- La Loi N°2013-546 du 30 Juillet 2013 Relative aux Transactions Electroniques

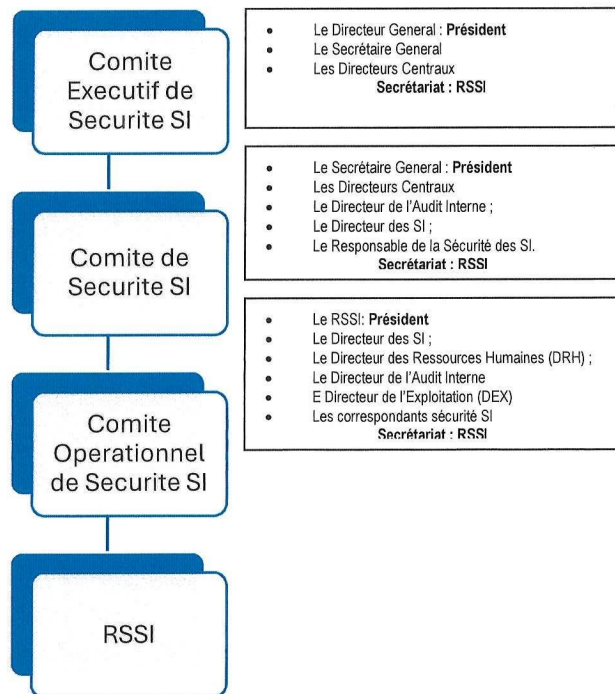
1.4.2. Au niveau international

Au niveau international, les textes suivants sont applicables :

- Convention de l'Union Africaine sur la cybersécurité et la protection des données à caractère personnel du 27 juin 2014
- Directive C/DIR/1/0811 du 19 août 2011 portant lutte contre la cybercriminalité dans l'espace de la Communauté Economique Des Etats de l'Afrique de l'Ouest (CEDEAO)

2. RESPONSABILITÉS ET GOUVERNANCE

2.1. Synthèse de l'organisation



2.2. Comité Exécutif de Sécurité SI

Le Comité Exécutif valide l'organisation et les moyens à mettre en place pour gérer et coordonner les actions de sécurité, sur proposition du Comité de Sécurité.

Plus spécifiquement, le Comité Exécutif a pour mission de :

- Assurer l'inclusion des valeurs et objectifs institutionnel dans la gestion de la sécurité de CI-ENERGIES ;
- Etablir les objectifs annuels en matière de sécurité de CI-ENERGIES ;
- S'assurer que les revues annuelles de sécurité ont lieu ;
- Fournir les ressources adéquates ;
- Contrôler la contribution du processus de gestion de la sécurité de CI-ENERGIES aux métiers ;
- Approuver les projets majeurs de sécurité de CI-ENERGIES ;
- Communiquer avec les parties prenantes externes.

Le Comité Exécutif est composé de :

- Le Directeur Général de CI-ENERGIES ;
- Le Secrétaire Général de CI-ENERGIES
- Les Directeurs Centraux

Le Comité exécutif est présidé par le DG de CI-ENERGIES.

Le secrétariat est assuré par le RSSI de CI-ENERGIES.

2.3. Le Comité de Sécurité du SI

Le Comité de Sécurité se réunit régulièrement pour :

- Faire le point sur le niveau de sécurité des SI ;
- Evaluer le niveau de conformité et de respect de la Politique de Sécurité au sein de CI-ENERGIES ;
- Coordonner les plans d'action associés à la sécurité SI ;
- Evaluer le niveau d'exécution des feuilles de routes issues des plans d'action ;
- Délibérer sur les points de décisions soumis par le Comité Opérationnel de sécurité ;
- Proposer éventuellement de nouvelles orientations au Comité de Exécutif.

Le Comité de Sécurité est composé de :

- Le Secrétaire Général de CI-ENERGIES ;
- Les représentants des Directeurs Centraux ;
- Le Directeur de l'Audit Interne ;
- Le Directeur des Systèmes d'Information ;
- Le Responsable de la Sécurité des SI.

Ce comité de sécurité est présidé par le Secrétaire Général de CI-ENERGIES.

Le secrétariat du Comité de Sécurité est assuré par le RSSI de CI-ENERGIES.

2.4. Le Comité Opérationnel de sécurité du SI

Le Comité Opérationnel a pour mission de :

- Assurer la mise en œuvre des mesures de sécurité de la politique de sécurité de CI-ENERGIES
- Promouvoir la cohérence de la mise en œuvre et la gestion de la documentation au sein de CI-ENERGIES
- Traiter les non-conformités et assurer une amélioration continue
- Rendre compte au Comité de Sécurité

Le Comité Opérationnel est composé de :

- Le RSSI de CI-ENERGIES
- La Direction de l'Audit Interne
- La Direction des Systèmes d'Information
- La DRH
- Les correspondants sécurité SI

Le Comité Opérationnel de sécurité du SI est présidé par le RSSI qui en assure également le secrétariat. 

Le Comité opérationnel peut être élargie à toute autre structure sur proposition du RSSI avec l'approbation du Comité de Sécurité.

2.5. Le RSSI de CI-ENERGIES :

Le RSSI de CI-ENERGIES (RSSI) :

- Est force de propositions auprès du Comité de Sécurité de l'Information ;
- Préside le Comité Opérationnel de sécurité de l'information ;
- Elabore les indicateurs de sécurité internes ;
- Participe aux groupes de travail relatifs à la Sécurité des Systèmes d'Information ;
- Participe aux comités de pilotage des projets de sécurité informatique ;
- A la charge du contrôle de l'application des règles définies dans la politique de sécurité, et des procédures associées ;
- Est impliqué dans les principaux projets de CI-ENERGIES pour qu'y soient traitées les problématiques de sécurité ;
- A en charge l'organisation de la sensibilisation du personnel aux questions de sécurité du Système d'Information ;
- A la responsabilité du Centre de Gestion des Operations de Sécurité appelé SOC
- Se tient informé de l'actualité relative à la sécurité du Système d'Information, notamment relayée par les organismes officiels ;
- Propose des améliorations de sécurité du Système d'Information ;
- A la responsabilité de développer les plans d'audit et d'évaluation du SMSI.

2.6. Correspondant Sécurité SI

Le correspondant sécurité SI a pour mission, en appui au RSSI et a son équipe, de :

- Assurer l'application de la sécurité de la politique de sécurité du SI
- Coordonner la mise en œuvre de la Politique de Sécurité à tous les échelons et domaines au sein de sa structure administrative
- Promouvoir et faire connaître la politique de sécurité en relation avec sa structure administrative
- Être de relai avec le RSSI de CI-ENERGIES auprès de sa structure administrative

Le correspondant sécurité est désigné dans les structures clientes de CI-ENERGIES pour lequel le Comité de Sécurité des SI considère que le risque inhérent de cybersécurité peut être systémique pour l'écosystème placé sous la responsabilité de CI-ENERGIES. 

2.7. Les experts en sécurité de l'information

- Forces de proposition auprès du RSSI ;
- Implémentation des politiques sectorielles et contrôles afférents à leurs domaines d'expertise ;
- Avis d'experts et soutien aux autres domaines et experts dans la mise en œuvre de la PSI ;
- Gestion des rapports et tableaux de bord ;
- Participation à la réponse aux incidents ;
- Revue et amélioration continue des processus ;
- Planification des ressources, plan de formation etc.

2.8. Tous les Employés :

Tous les employés doivent respecter les procédures de sécurité et signaler toute anomalie ou incident de sécurité.

2.9. Tableaux de bord

CI-ENERGIES met en place un tableau de bord sur la sécurité des systèmes d'information pour lui permettre de suivre l'état de la sécurité, de communiquer efficacement avec les parties prenantes et d'améliorer continuellement les mesures de sécurité.

A cet effet, le RSSI transmettra à la Direction, au moins une fois par mois, un rapport sur l'état de la sécurité et un rapport détaillé sur les incidents incluant la nature de l'incident, les mesures prises et les actions correctives.

Lors des réunions du Comité de sécurité, un rapport sur l'état de la sécurité sera présenté aux membres.

A la fin de l'année, un rapport annuel est établi et mis à la disposition de la Direction générale.

3. LES PRINCIPES DIRECTEURS

La PSI de CI-ENERGIES s'articule autour de principes directeurs, à savoir :

- Une approche holistique de la sécurité de l'information ;
- La responsabilisation de tous les acteurs ;
- La proportionnalité des mesures de sécurité par rapport aux enjeux et menaces ;
- La proactivité ;
- La visibilité ;
- L'amélioration continue ;
- Principes de conformité, de cohérence, d'efficacité et de pérennité
- L'exception documentée

3.1. Approche holistique

La gouvernance de la sécurité de l'information fait partie intégrante de la gouvernance d'entreprise. A ce titre, elle est exercée par les Autorités de CI-ENERGIES qui, d'une part, définissent les orientations stratégiques et fixent les objectifs et, d'autre part, s'assurent de l'atteinte des objectifs fixés, la maîtrise des risques et l'utilisation efficace et efficiente des ressources.

L'approche holistique se traduit par la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI), en harmonie avec la vision stratégique de CI-ENERGIES.

La sécurité de l'information doit permettre une protection appropriée de tous les actifs du patrimoine informationnel de CI-ENERGIES, à tous les stades de leur cycle de vie. A cet égard, elle doit être alignée sur les stratégies de l'Institution et intégrée à ses processus critiques.

L'application de la PSI doit se matérialiser par l'adoption de mesures cohérentes et une mutualisation des ressources mises en œuvre. Les mesures de sécurité doivent être intégrées de manière à fournir une protection résiliente : en cas de défaillance d'une mesure, les mesures adjacentes doivent permettre d'assurer le maintien du niveau de sécurité adéquat.

3.2. Responsabilisation

Quelle que soit sa fonction, le facteur humain est souvent considéré comme le maillon le plus vulnérable de la sécurité de l'information. Par conséquent, il est primordial d'amener tous les acteurs à prendre conscience de leurs rôles et responsabilités dans la sécurisation du patrimoine informationnel de CI-ENERGIES. Chacun doit, à son niveau, contribuer à la prévention, la détection et la correction des dysfonctionnements

susceptibles d'affecter les actifs d'information et dont les conséquences sont dommageables à CI-ENERGIES.

Aussi :

- Chaque manager est responsable de la mise en œuvre de la politique de sécurité de l'information dans sa structure administrative ;
- Chaque employé est informé de ses obligations réglementaires et contractuelles ainsi que des mesures mises en place pour assurer la sécurité du SI ;
- Chaque employé est responsable des informations et ressources qu'il manipule dans le cadre de ses fonctions ;
- Tout employé doit être informé des dispositions générales de collecte d'informations personnelles selon la législation applicable ;
- Tout employé en déplacement ou expatrié doit se conformer aux règles de sécurité préconisées par l'entreprise ;
- Tout employé qui viole intentionnellement les déclinaisons de la politique de sécurité de l'information s'expose à des sanctions disciplinaires, voire pénales, conformément aux obligations issues des dispositifs légaux ou réglementaires ainsi que celles inhérentes au règlement intérieur, aux contrats de travail et à l'ensemble des textes opposables.

3.3. Proportionnalité

La conception des mesures visant la sécurité de l'information doit être guidée par la recherche du juste niveau de sécurité, grâce à une approche par les risques. La démarche adoptée consiste à identifier les besoins de sécurité, en partant des enjeux et des menaces, en vue de définir les moyens optimaux (humains, organisationnels et techniques) à mettre en œuvre pour atteindre le niveau de sécurité adéquat et s'y maintenir.

3.4. Proactivité

La gestion de la sécurité de l'information doit être proactive. En effet, la maîtrise des risques liés aux systèmes d'information nécessite une bonne anticipation des mutations de l'environnement, notamment les changements organisationnels, l'apparition de nouvelles menaces, ainsi que les évolutions technologiques, législatives et réglementaires.

En outre, les activités de contrôle doivent être orientées vers la prévention des risques. A cet égard, les besoins en contrôle dans les processus informatisés doivent systématiquement être formalisés, en se basant sur les exigences de sécurité (disponibilité, intégrité, confidentialité et imputabilité). *✍*

Nonobstant les mesures de prévention, une capacité de réponse aux incidents adaptée aux enjeux doit être maintenue, en vue de permettre à CI-ENERGIES de faire face aux événements, prévisibles ou non, susceptibles de compromettre l'atteinte de ses objectifs.

3.5. Visibilité

Il est primordial que, dans l'exercice de leurs fonctions, les acteurs de la sécurité de l'information soient en mesure de prendre à temps les décisions appropriées. C'est pourquoi chacun doit disposer de la visibilité nécessaire à la prise des décisions qui lui incombent, en se fondant sur des informations pertinentes, fiables et disponibles en temps opportun.

Par conséquent, la gestion de la sécurité de l'information nécessite la définition systématique de points de surveillance fondamentaux, d'indicateurs et de tableaux de bords permettant d'assurer la supervision, le reporting, ainsi que le suivi requis aux niveaux stratégique, managérial et opérationnel.

L'assurance d'une bonne visibilité reposera sur la mise en place des flux d'information et canaux de communication nécessaires, ainsi que sur une documentation pertinente couvrant tout le cycle de vie des différents processus qui concourent à la sécurité de l'information.

3.6. Amélioration continue

Pour une prise en compte adéquate des évolutions, la sécurité doit être agile et le niveau de sécurité adapté maintenu en permanence. A cet effet, CI-ENERGIES doit s'inscrire dans une logique d'amélioration continue, en s'alignant sur des pratiques et standards reconnus et utilisés à l'échelle internationale.

3.7. Principe de cohérence

La sécurité globale d'un système est toujours celle du composant le plus faible. La mise en œuvre efficace de services de sécurité repose sur un principe de cohérence. En vertu de ce principe, les services de sécurité offerts garantissent un niveau de sécurité homogène dans tous les domaines de la prévention, de la détection et de la protection. La recherche de ce niveau de sécurité cohérent doit donc rester la règle. Les règles énoncées par la politique de sécurité sont systématiquement suivies afin de satisfaire à ce principe.

3.8. Principe d'efficacité

L'efficacité d'un service de sécurité se mesure en fonction de la capacité de ce service à prévenir, à détecter un incident et à réagir pour s'en protéger lorsqu'il survient. Cette capacité de prévention, détection, protection ou réaction dépend essentiellement de la facilité de mise en œuvre de ce service de sécurité par le personnel. Avant tout, elle doit être à la hauteur du risque encouru. Dans cet esprit, les règles définies par la politique de

sécurité permettent de disposer d'un service efficace de sécurité, c'est-à-dire adapté aux risques encourus, aux métiers du personnel et à l'organisation.

3.9. Principe de pérennité

La politique de sécurité s'inscrit dans un processus visant à gérer et à suivre dans le temps la sécurité du système d'information. Les règles qu'elle énonce s'appuient donc sur des principes pérennes. Il doit en être de même pour les moyens de sécurité mis en œuvre, qui doivent offrir des garanties d'évolutivité dans le temps, d'adaptabilité à l'apparition de nouveaux risques et de maintenance à un coût raisonnable.

3.10. Principes de conformité

La politique de sécurité constitue la base d'un référentiel sur lequel s'appuie l'ensemble des procédures et des mesures définies par chaque structure pour garantir la sécurité des systèmes d'information. Ce référentiel est exploité et alimenté par chaque Direction. Dans cet esprit, les Directions se conforment à l'ensemble des règles énoncées par la politique de sécurité pour la définition de leurs procédures de sécurité et la mise en œuvre des mesures adaptées.

3.11. Principe d'exception documenté

Le principe est de considérer l'existence d'exceptions sur le terrain à l'application des règles de sécurité formulées pour l'actif de référence.

Les environnements pour lesquels il n'est pas raisonnable d'exiger une stricte conformité à toutes les exigences formulées pour l'actif de référence sont soumis au « principe d'exception documentée ».

Ce principe, dit « principe d'exception documentée », est décrit ici :

Par défaut, tout actif possédant des caractéristiques pour lesquelles une procédure de sécurité d'un actif de référence est définie doit respecter les exigences de cette procédure.

Dans le cas où cette conformité n'est pas envisageable (pour des raisons économiques notamment), l'actif peut faire l'objet de mesures ou de procédures allant en deçà, à condition qu'un dossier documenté soit fourni, précisant dans quelle mesure les règles en place sont optimales par rapport à l'environnement effectif et aux objectifs des mesures théoriquement prévues.

4. PRINCIPES DE SECURITE

Les principes de sécurité de CI-ENERGIES sont issus de la norme internationale ISO/CEI 27002:2022 (Sécurité de l'information, cybersécurité et protection de la vie privée — Mesures de sécurité de l'information). Ces principes sont regroupés en 3 champs d'action principaux :

- Les principes organisationnels,
- Les principes de mise en œuvre,
- Les principes techniques.

4.1. Les principes de mise en œuvre

4.1.1. La gestion des risques SSI

Afin de protéger son système d'information, CI-ENERGIES doit connaître, analyser et évaluer les risques auxquels il est exposé, et agir en conséquence. Ainsi CI-ENERGIES procédera régulièrement à l'identification et l'évaluation des risques pour élaborer un plan de traitement approprié. L'analyse des risques se fera en conformité avec la norme ISO 27005. Le traitement des risques consiste en la mise en place de mesures pour atténuer les risques identifiés, telles que des contrôles techniques, organisationnels et de gestion.

Le choix des mesures de sécurité est guidé par l'appréciation du risque. Les Autorités décident du traitement d'un risque en fonction des conséquences sur :

- La remise en question de l'exercice des missions fondamentales de CI-ENERGIES ;
- L'image de l'Institution ou l'altération de la confiance des autorités de tutelle, des partenaires, des acteurs du système monétaire, bancaire et financier, ainsi que du public ;
- La perturbation de l'exécution des opérations ou la compromission de la continuité d'activité ;
- Les pertes financières directes ou indirectes ;
- Le non-respect des obligations statutaires, législatives, réglementaires et contractuelles.

L'intégration de la prévention des risques dans la culture de l'Institution est un axe majeur de la stratégie de sécurité de l'information de CI-ENERGIES.

4.1.2. La sécurité et le cycle de vie du logiciel

Des mesures de sécurité doivent être respectées durant tout le cycle de vie des logiciels. Ces mesures sont applicables dans le cas de nouvelles acquisitions, comme dans le cas de changements sur des logiciels existants. Les règles de développement sécurisé

doivent être respectées pour les développements internes. Les environnements de développement, de test et de production sont séparés. Les données de développement et de test ne contiennent pas de données réelles de clients, employés, fournisseurs ou autres tiers.

Les applications font l'objet d'audit de sécurité avant mise en production.

4.1.3. Conformité et audits

A travers la mise en œuvre de cette politique de sécurité, CI-ENERGIES s'assure la conformité avec les lois et réglementations en vigueur.

Des audits internes ou externes réguliers seront menés pour vérifier la conformité avec la politique de sécurité.

4.1.4. Les aspects humains

CI-ENERGIES met en œuvre des procédures de sécurité appropriées avant l'embauche, durant la période d'emploi et à la cessation d'activité pour s'assurer que les employés et toutes les personnes autorisées à accéder au système d'information sont dignes de confiance et qu'ils respectent la politique de sécurité.

Les contrats de travail ou de prestations mentionnent les obligations des employés ou des tiers en matière de sécurité informatique et les sanctions en cas de manquement.

4.1.5. La gestion des actifs

Tous les actifs physiques et logiciels de CI-ENERGIES doivent être inventoriés afin d'identifier leurs responsables (notion de propriété d'un actif) et affecter un niveau de protection adéquat selon la nature de l'information manipulée et/ou stockée.

Les actifs informationnels doivent faire l'objet d'un inventaire maintenu à jour et d'une valorisation, en vue de la détermination des besoins en sécurité selon les critères retenus par CI-ENERGIES (disponibilité, intégrité, confidentialité et auditabilité).

Les modalités de traitement des informations sont définies en fonction de leur sensibilité et couvrent au minimum l'étiquetage, la copie, la distribution, le stockage et la mise au rebut.

4.1.6. La planification de la continuité des activités

CI-ENERGIES ne peut pas se permettre une interruption prolongée de son système d'information. Afin de se prémunir du risque d'interruption de service, CI-ENERGIES se dote d'un plan de continuité d'activités (PCA). Ce PCA vise à garantir la reprise des activités dans les délais nécessaires à l'exécution des missions de l'entreprise, et à définir l'ensemble des plans et moyens nécessaires pour satisfaire aux exigences de l'entreprise en matière de continuité des activités. Le PCA doit être testé et maintenu en conditions opérationnelles.

Une politique de sauvegarde régulière pour les informations et les logiciels essentiels est définie pour les activités de l'entreprise, conformément aux obligations légales en vigueur et aux exigences de la PSI, appliquées aux documents numériques et physiques.

4.1.7. La gestion des incidents

CI-ENERGIES mettra en place un processus de gestion des incidents qui permette de :

- Détecter, signaler et répondre aux incidents de sécurité.
- Analyser post-mortem les incidents pour identifier les causes profondes et mettre en œuvre des actions correctives.

4.1.8. La sensibilisation et la formation

Les utilisateurs sont souvent le maillon faible de la chaîne de sécurité.

Ainsi, afin de s'assurer une bonne compréhension et partant une bonne mise de la PSI par les utilisateurs, CI-ENERGIES va offrir des formations régulières sur les bonnes pratiques de sécurité des informations et promouvoir une culture de sécurité à tous les niveaux de l'organisation à travers des campagnes de sensibilisation.

4.1.9. L'exploitation

CI-ENERGIES préserve la sécurité de l'environnement de production en mettant en œuvre des mesures de protection de ses actifs, de détection des intrusions et de maintien de la sécurité opérationnelle.

Le niveau de sécurité opérationnelle sera maintenu en appliquant les derniers correctifs de sécurité, en utilisant des logiciels de protection contre les programmes et actes malveillants etc.

Toutes les tâches et activités d'exploitation feront l'objet de procédures documentées.

4.1.10. Infogérance

L'infogérance correspond au fait que des sociétés extérieures, chargées de gérer une partie de l'informatique, ont accès au système d'information depuis l'extérieur ou l'intérieur. Un contrat entre CI-ENERGIES et chaque société doit clairement préciser les droits d'accès, les engagements de responsabilités et l'imputabilité en cas d'incident. Des mécanismes permettant de s'assurer du respect des limites d'intervention doivent être mis en œuvre dans la mesure du possible.

L'externalisation de la gestion d'exploitation d'un composant critique pour le système d'information doit faire l'objet d'une analyse de risque spécifique qui sera soumise à l'appréciation du Comité de Sécurité après avis du RSSI. 

4.1.11. Les aspects physiques

CI-ENERGIES se dote d'une protection contre les menaces physiques et environnementales telles que les catastrophes naturelles et autres menaces physiques, intentionnelles ou non intentionnelles, impactant l'infrastructure.

CI-ENERGIES met en œuvre des mesures appropriées incluant les contrôles d'accès, la vidéo surveillance et des systèmes de détection d'intrusion physique, pour empêcher et/ou détecter l'accès physique non autorisé.

4.2. Les principes techniques

4.2.1. Gestion des identités et des accès

Un contrôle de l'accès physique et logique au matériel et aux logiciels doit être mis en place pour permettre de garantir un niveau élevé de sécurité de ces derniers. Ainsi toute personne accédant au SI devra avoir un identifiant unique et nominatif auquel est associé un profil limité strictement aux attributions de son poste.

La séparation des tâches devra être respectée dans la définition des profils et CI-ENERGIES met en place une procédure stricte de gestion des identifiants et des accès qui régit l'ajout, la modification et la suppression des droits d'accès.

Les règles de gestion des authentifiants doivent donner l'assurance que les mots de passes acceptés sont de qualité (non évidents, difficiles à deviner) et qu'elles permettent de protéger les systèmes des attaques de mots de passe par balayage de dictionnaire. Et empêcher l'accès non autorisé aux systèmes.

4.2.2. Sécurité des applications

La sécurité doit être prise en compte à toutes les étapes d'un projet, interne ou externe, lié au système d'information de CI-ENERGIES. A cet effet, un dossier de sécurité doit accompagner chaque projet et préciser les objectifs, les méthodes et les mesures préconisées. En particulier, les applications informatiques de gestion et les applications internet, doivent être sécurisées, en cohérence avec la sensibilité des informations traitées et échangées. Chaque dossier de sécurité doit être approuvée par le RSSI.

Dans le cadre du développement et de la maintenance des applications, Il est mis en place des environnements de développement, de recette et de production, différenciés, gérés avec des règles précises. Pour les applications les plus sensibles, il doit également être mis en œuvre un environnement de préproduction strictement identique à l'environnement de production.

Avant la mise en production d'une application il est impératif de mettre en place des contrôles d'accès logiques à l'application ou au système, s'assurer que les éléments sécurité sont pris en compte par les administrateurs système et que les procédures d'exploitation et d'administration sécurisées sont bien établies et utilisables. \$

Les ressources (logiciels, fichiers, documentation) utilisées dans le cadre du développement d'une application doivent être la propriété exclusive de CI-ENERGIES.

4.2.3. La sécurité des réseaux

L'administration du réseau informatique est placée exclusivement sous la responsabilité exclusive du Directeur des Systèmes d'Information et par délégation aux administrateurs systèmes et réseaux de CI-ENERGIES.

Les systèmes d'information doivent être protégés vis-à-vis de l'extérieur à l'aide de filtres d'accès appliqués sur les équipements en tête de son réseau. Ces filtres s'appliquent tant sur les flux réseaux entrants que sur les flux sortants. Les flux entrants concernent principalement l'accès aux serveurs. L'accès extérieur aux postes de travail et aux équipements doit demeurer l'exception et être justifié en termes de besoins et de compétences.

La politique de définition des filtres d'accès décrivant les flux réseaux entrants est systématiquement du type « tout ce qui n'est pas explicitement autorisé est interdit ».

Les serveurs doivent être protégés spécifiquement vis-à-vis des postes de travail et des autres serveurs.

Les serveurs potentiellement accessibles de l'extérieur feront l'objet d'une surveillance accrue. L'accès externe aux serveurs s'effectue à travers des connexions dédiées et chiffrées.

L'accès au réseau sans-fil doit faire l'objet d'un contrôle spécifique et n'être autorisé qu'après authentification du terminal et de l'utilisateur.

L'accès aux réseaux locaux et aux services locaux doivent être subordonnés à une authentification et une autorisation. Tous les accès doivent être journalisés.

4.2.4. La sécurité des systèmes industriels

Toutes les technologies et installations mises en œuvre dans le cadre de la production, le transport, le stockage et la distribution de l'électricité, ainsi que pour le contrôle des processus support associés doivent être conformes à la norme ISO/IEC 27019:2024 et/ou ISA/IEC 62443.

Il s'agit notamment des technologies centralisées et distribuées de contrôle, de surveillance et d'automatisation des processus et les systèmes d'information utilisés pour leur exploitation, y compris :

- Les dispositifs de programmation et de paramétrage ;
- Les technologies de communication utilisées dans le domaine du contrôle des processus dont les réseaux, la télémétrie, les applications de téléconduite et les technologies de contrôle à distance ;

- Les dispositifs de mesure ;
- Les systèmes de protection et de sûreté numériques, tels que les relais de protection, les automates programmables de sûreté (PLC) ou les régulateurs d'urgence ;
- Tous les logiciels et applications installées sur les systèmes et sous-systèmes déployés ;
- Tous les locaux hébergeant les équipements et les systèmes et sous-systèmes déployés ;
- Les systèmes de maintenance à distance pour les systèmes et sous-systèmes déployés ;
- Etc.

4.2.5. L'administration des serveurs et des postes de travail

L'administration des serveurs est placée sous la responsabilité des administrateurs systèmes par délégation du Directeur des Systèmes d'Information.

L'administration des postes de travail individuels est placée sous la responsabilité des administrateurs systèmes et réseaux. L'administration des postes par les utilisateurs eux-mêmes doit demeurer l'exception et être justifiée en termes de besoins et de compétences. Les administrateurs systèmes et réseaux peuvent intervenir à distance pour des opérations de maintenance sur le poste de travail d'un utilisateur après l'en avoir averti et en respectant les principes de la charte informatique.

4.2.6. La journalisation

Tous les événements ayant un rapport avec la gestion de la sécurité doivent être enregistrés au niveau du réseau, des systèmes et des applications. Les journaux d'événements doivent être protégés contre les accès non autorisés et la falsification.

Les journaux doivent être tenus à jour et revus périodiquement.

4.2.7. Les infrastructures de gestion des clés cryptographiques

Le chiffrement constitue un moyen privilégié de protection des données. Son emploi est obligatoire pour le stockage et l'échange de données, en particulier celles dites sensibles.

Les produits utilisés dans le cadre du chiffrement doivent faire l'objet d'une approbation au sein de CI-ENERGIES. A cet effet, un répertoire des algorithmes, tailles de clés de chiffrement et produits approuvés doit être tenu à jour par le RSSI.

Tout chiffrement implique la mise en œuvre de procédures permettant de restituer en toutes circonstances les données en clair, y compris en cas de perte du secret permettant de les déchiffrer. A cet effet, CI-ENERGIES peut procéder par séquestre de clés, procédure de recouvrement, voire maintien d'une copie en clair. §

Le RSSI de CI-ENERGIES doit informer les utilisateurs de l'importance d'un renouvellement régulier des clés cryptographiques. L'archivage de données chiffrées doit faire l'objet de mesures de conservation particulières.

4.2.8. Cyber surveillance et signaux de compromission

CI-ENERGIES se donne les moyens de collecter l'information pertinente pour déterminer les signaux d'une compromission et/ou d'un danger imminent. Cette veille peut se faire par la souscription à des sources d'information spécialisées, payantes ou communautaires.

La sécurité des systèmes d'information exige de pouvoir surveiller le trafic sur le réseau et tracer les actions effectuées. Les dispositifs mis en œuvre doivent être conformes à la réglementation en vigueur et respecter les principes de proportionnalité (adaptation du niveau des moyens à l'enjeu effectif de la sécurité) et de transparence (information des partenaires sociaux et utilisateurs).

Par ailleurs l'utilisation de certains matériels ou logiciels peut s'avérer préjudiciable à la sécurité des systèmes d'information. Ces produits font l'objet d'identification et de « mises en garde » de la part du RSSI, visant soit des recommandations d'utilisation, soit une interdiction pure et simple.

4.2.9. La sécurité physique

Les actifs de CI-ENERGIES doivent être protégés en fonction de la sensibilité des informations qu'ils produisent, hébergent ou transportent. Aussi, les différents locaux doivent être analysés selon l'échelle de sensibilité suivante :

- Niveau 4 : Qualifie les locaux ou bâtiments dont la destruction ou compromission pourrait nuire au fonctionnement de l'ensemble de l'entreprise.
- Niveau 3 : Qualifie les locaux ou bâtiments dont la destruction ou compromission pourrait nuire au fonctionnement de tout un service ou impacter partiellement sur plusieurs sites.
- Niveau 2 : Qualifie les locaux ou bâtiments dont la destruction ou compromission pourrait nuire au fonctionnement de toute une équipe, d'une zone ou d'un étage.
- Niveau 1 : Tous les autres locaux, en particulier les circulations et bureaux.

Un tableau doit mettre en correspondance, au cas par cas et pour chaque axe, les niveaux de sensibilité avec les mesures de sécurité acceptables pour chaque niveau. 

Les axes des mesures de sécurité physique sont :

- Le contrôle d'accès physique ;
- La détection et la protection incendie ;
- La protection contre les dégâts des eaux ;
- La climatisation ;

- La sécurisation de l'alimentation électrique et des courants faibles ;
- La protection contre la foudre ;
- Le contrôle de l'humidité ambiante ;

5. LA MISE EN APPLICATION ET LE SUIVI DE LA POLITIQUE DE SECURITE

5.1. Validation de la politique de sécurité

La définition de la politique de sécurité, et ses évolutions, reposent sur une organisation respectant le principe de la séparation des pouvoirs (Décision, Mise en application et Contrôle). La décision de mise en œuvre est du ressort de la Direction Générale. Le RSSI assure la mise en application. Le comité de sécurité assure le contrôle et propose les évolutions.

5.2. Diffusion et classification de la politique de sécurité

La politique de sécurité est un document interne à CI-ENERGIES, accessible par l'ensemble du personnel. Il est diffusé à l'ensemble des directeurs, qui ont la charge de le transmettre à leurs responsables de service et à l'ensemble du personnel.

En aucun cas, il ne peut être diffusé à l'extérieur de CI-ENERGIES sans accord préalable du RSSI.

5.3. Evolution de la politique de sécurité

Une révision de la PSI peut s'avérer nécessaire à la suite d'incidents de sécurité, de changements importants dans le SI ou de modifications réglementaires. Cette révision exceptionnelle sera soumise à la validation du Comité de sécurité du SI.

Par ailleurs, le comité de Sécurité du SI, à son initiative ou sur proposition du RSSI, peut à tout moment revoir et faire évoluer la politique de sécurité avec l'approbation de la Direction Générale.

Chaque Direction est tenue d'informer le comité de sécurité des anomalies constatées vis à vis de la politique de sécurité. Ce comité les étudie et, si besoin est, propose à la Direction Générale les évolutions adéquates.

5.4. Gestion des dérogations

Par principe, il ne doit pas exister de dérogation à la politique de sécurité. Les seules dérogations possibles sont du ressort de la Direction Générale ou du comité de sécurité en fonction de l'urgence et de l'importance de la situation. §