POLITIQUE DE SÉCURITÉ DES SYSTÈMES D'INFORMATION
(PSSI)

BIOÉNERGIE TECH – Zone classifiée « Confidencial »

Projet SpainTurbine (Armée espagnole)

Document interne – Diffusion restreinte

Référence : PSSI-BET-ST-2026-V1.0

Date d'émission : 19 mai 2026

Émetteur : Responsable de la Sécurité des Systèmes d'Information (RSSI)

Validation : Direction Générale BIOÉNERGIE TECH

Sommaire

Suivi des versions

Version	Date	Auteur	Validation	Nature de la modification
1.0	19/05/2026	RSSI	DG / DPO	Création initiale de la PSSI – zone classifiée Confidencial

Classification du présent document : DIFFUSION RESTREINTE.

Le présent document est diffusé exclusivement au Comité de Direction de BIOÉNERGIE TECH, au RSSI, à l'administrateur du système d'information ainsi qu'aux personnels nominativement habilités sur le projet SpainTurbine. Toute reproduction, transmission à un tiers non habilité ou sortie du périmètre de l'entreprise est strictement interdite et expose son auteur aux sanctions disciplinaires et pénales prévues par la loi française et par les engagements contractuels pris envers l'Armée espagnole.

Préambule

Objet de la PSSI

La présente Politique de Sécurité des Systèmes d'Information (ci-après « PSSI ») définit les principes, règles et dispositifs de sécurité que BIOÉNERGIE TECH est tenue d'appliquer pour la conception, l'exploitation et le maintien en condition de sécurité du système d'information dédié à la zone classifiée « Confidencial » destinée au projet SpainTurbine.

Elle traduit la volonté de la Direction Générale d'assurer la confidentialité, l'intégrité, la disponibilité et la traçabilité (CID-T) des informations classifiées détenues, traitées ou échangées dans le cadre du contrat de fourniture de 120 micro-turbines mensuelles pour drones militaires conclu avec l'Armée espagnole.

Périmètre d'application

La PSSI s'applique à l'ensemble des actifs, personnels et tiers intervenant sur la zone classifiée « Confidencial » de BIOÉNERGIE TECH (Chambéry) : les trois postes utilisateurs du projet, le poste de mise à jour, le poste de chiffrement/déchiffrement, la salle serveur dédiée (serveur principal PowerEdge R470 et son redondant), les équipements réseau (switch Cisco Catalyst 9200, pare-feu Cisco Secure Firewall 1120), les périphériques de sécurité (station blanche S3Box Hogo, coffre-fort Fichet-Bauche Carena, lecteurs biométriques HID Signo 25B, YubiKey C NFC, caméra Axis M4216-V) et l'ensemble des supports de sauvegarde LTO-8.

Cadre normatif et réglementaire

La PSSI s'inscrit dans le respect des textes suivants :

- Règlement (UE) 2016/679 dit « RGPD » et Loi française n° 78-17 « Informatique & Libertés » pour les données à caractère personnel des salariés et des intervenants tiers.
- Directive (UE) 2022/2555 dite « NIS 2 » transposée en droit français – BIOÉNERGIE TECH étant qualifiée d'entité essentielle au titre de son activité dans la chaîne d'approvisionnement de la défense.
- Instruction Générale Interministérielle n° 1300 sur la protection du secret de la défense nationale (référentiel équivalent espagnol pour la classification « Confidencial »).
- Référentiel ANSSI EBIOS Risk Manager pour la conduite de l'analyse de risques.
- Norme ISO/IEC 27001:2022 et code de bonnes pratiques ISO/IEC 27002:2022.
- Code pénal, articles 413-9 et suivants (atteintes au secret de la défense nationale).

Caractère normatif et opposabilité

La PSSI a un caractère normatif. Le respect de ses dispositions s'impose à tout collaborateur, sous-traitant, visiteur ou prestataire qui accède – ou pourrait accéder – à la zone classifiée. Tout manquement avéré expose son auteur à des sanctions disciplinaires graduées, contractuelles et, le cas échéant, pénales. Le présent document est revu annuellement par le RSSI, et systématiquement à la suite d'un incident majeur, d'un changement structurel d'architecture, ou de l'évolution du cadre réglementaire applicable.

1. Contexte, environnement et analyse des risques

1.1 Environnement de l'organisation et spécificités du système d'information

1.1.1 Contexte économique et industriel

BIOÉNERGIE TECH est une PME industrielle de 49 collaborateurs implantée à Chambéry, spécialisée dans la conception et la fabrication de cellules et modules de batteries innovantes ainsi que de turbines mini-hydrauliques. Elle évolue dans un environnement industriel à forte coactivité (industries chimiques, métallurgiques et logistiques voisines à moins de 100 mètres) et adresse une clientèle mixte civile et défense (DGA, ANSC, AéroBat Innovation, AlpEnergy Réseaux, SpainTurbine, etc.).

La signature du contrat avec SpainTurbine – 120 micro-turbines mensuelles à destination de drones militaires de l'Armée espagnole pour un montant annuel de 1,2 M€ – place de facto BIOÉNERGIE TECH dans la chaîne d'approvisionnement de la défense et l'expose au régime de protection des informations classifiées « Confidencial ».

1.1.2 Spécificités du système d'information de la zone classifiée

Conformément aux exigences contractuelles et au principe « rien ne doit sortir, rien ne doit entrer sans validation », un système d'information dédié, strictement cloisonné et physiquement isolé du SI corporate (« air-gap »), est déployé pour le projet SpainTurbine. Ses caractéristiques principales, telles que définies par le Dossier d'Architecture Technique (DAT) de BIOÉNERGIE TECH, sont les suivantes :

- Cloisonnement physique et logique total : aucune interconnexion réseau avec le SI principal, aucun accès direct à Internet depuis les postes opérationnels. Toute communication extérieure transite par le poste de mise à jour et la station blanche.
- Architecture matérielle dimensionnée : switch unique Cisco Catalyst 9200, pare-feu Cisco Secure Firewall 1120, deux serveurs Dell PowerEdge R470 (principal + redondance), trois postes utilisateurs HP Elite 800 G9, un poste dédié au téléchargement des mises à jour, un poste dédié au chiffrement/déchiffrement.
- Authentification forte : badge nominatif et YubiKey C NFC FIDO2 pour les employés projet ; double facteur badge + YubiKey pour l'administrateur sur la salle serveur ; deux lecteurs biométriques HID Signo 25B contrôlant l'accès au SAS puis au local sécurisé.
- Sauvegardes hors-ligne : lecteur LTO-8 HPE StoreEver Ultrium 30750, 15 cartouches IBM LTO-8, sauvegarde complète hebdomadaire et incrémentale quotidienne, dépôt des bandes dans le coffre-fort Fichet-Bauche Carena 120 L une fois par semaine.
- Journalisation et SIEM : pile ELK (Elasticsearch, Logstash, Kibana) centralisant l'intégralité des journaux d'événements ; la supervision Centreon n'est pas déployée, ELK étant jugé suffisant pour le périmètre.
- Contrôles complémentaires : verrous physiques sur les ports USB et RJ45, caméra IP Axis M4216-V sur le SAS d'accès, coffre-fort à six compartiments cloisonnés pour les supports sensibles, station blanche S3Box Hogo pour l'analyse de tout support amovible.
- PKI et Active Directory : authentification Kerberos/LDAPS, distribution des certificats par PKI interne, chiffrement SMB v3 pour les partages de fichiers, TLS interne pour l'ensemble des flux.

Le budget total des équipements de sécurité atteint 109 400,35 € HT, ce qui constitue un effort financier significatif pour une PME et impose un arbitrage permanent entre exigence sécuritaire maximale et viabilité économique (cf. chapitre 8.3).

1.2 Actifs primordiaux à protéger

L'analyse des biens essentiels au sens d'EBIOS RM identifie quatre catégories d'actifs primordiaux. Toute mesure prescrite par la présente PSSI doit pouvoir être rattachée à la protection d'au moins l'un de ces actifs.

Catégorie	Actif primordial	Critères de sécurité dominants	Niveau de classification
Informations	Plans, formulations, paramètres machines et spécifications techniques des micro-turbines drones SpainTurbine	Confidentialité, Intégrité, Traçabilité	Confidencial
Informations	Données à caractère personnel des 5 salariés habilités et des sous-traitants (habilitations, contrôles d'accès, biométrie)	Confidentialité, Intégrité (RGPD)	Sensible
Informations	Journaux d'événements ELK et enregistrements vidéo Axis M4216-V	Intégrité, Disponibilité, Traçabilité	Sensible
Processus	Fabrication, contrôle qualité et expédition des micro-turbines	Disponibilité, Intégrité	Critique
Processus	Sauvegardes LTO-8 et coffre-fort Fichet-Bauche	Confidentialité, Intégrité, Disponibilité	Critique
Image	Réputation contractuelle vis-à-vis de l'Armée espagnole, DGA et ANSC	Confidentialité (impact réputationnel)	Critique
R&D	Brevets, secrets de fabrication, alliages et électrochimie	Confidentialité, Intégrité	Confidencial

1.3 Analyse de risques EBIOS Risk Manager

L'analyse de risques s'appuie sur la méthode EBIOS Risk Manager publiée par l'ANSSI. Sa structure en cinq ateliers (cadrage, sources de risque, scénarios stratégiques, scénarios opérationnels, traitement) est appliquée à la nouvelle activité SpainTurbine. Ne sont restitués ici que les éléments synthétiques ; le rapport EBIOS RM complet constitue une annexe distincte du présent document.

1.3.1 Sources de risques et objectifs visés

Source de risque	Objectif visé	Motivation	Capacité
Service de renseignement étatique concurrent	Exfiltration des plans des micro-turbines	Avantage militaire/économique	Très élevée (APT)
Groupe cybercriminel	Rançongiciel sur le SI cloisonné	Gain financier	Élevée
Concurrent industriel	Vol de secrets de fabrication	Avantage commercial	Moyenne
Salarié ou prestataire malveillant	Sabotage, fuite d'information	Rancune, corruption, idéologie	Moyenne (initié)

Salarié négligent ou non sensibilisé	Divulgation accidentelle, perte de support	Erreur	Variable
Activiste / hacktiviste	Sabotage symbolique, défacement	Idéologie	Faible à moyenne

1.3.2 Scénarios stratégiques et événements redoutés

Événement redouté	Actif touché	Impact (G=Gravité, V=Vraisemblance)	Conséquences pour l'activité
Exfiltration des plans Confidencial par APT	Plans turbines, R&D	G=4 / V=3	Rupture contrat 1,2 M€/an, sanctions IGI 1300, perte habilitation
Compromission par chaîne d'approvisionnement (firmware, mises à jour, sous-traitants)	Postes, serveurs, station blanche	G=4 / V=3	Backdoor persistante, exfiltration silencieuse, atteinte à l'intégrité produit
Sabotage interne par un salarié habilité	Process fabrication, données	G=4 / V=2	Arrêt production, retard livraison, perte confiance armée espagnole
Rançongiciel rebondissant depuis le SI corporate	SI cloisonné par contagion via USB	G=3 / V=3	Indisponibilité prolongée, coûts de restauration
Perte ou vol d'une bande LTO-8 hors coffre	Sauvegardes Confidencial	G=4 / V=2	Fuite massive de données, notification ANSSI/CNIL/Armée
Phishing ciblé d'un employé habilité	Identifiants, machine	G=3 / V=4	Compromission initiale, élévation de privilèges
Indisponibilité prolongée du serveur principal	Disponibilité du SI	G=3 / V=2	Retard fabrication, pénalités contractuelles
Inondation ou incendie chez voisin CHEMICALIA/métallurgistes	Local sécurité, salle serveur	G=4 / V=2	Destruction matérielle, perte d'exploitation
Divulgation accidentelle d'une donnée (email, téléchargement)	Confidentialité	G=2 / V=4	Manquement RGPD/IGI 1300, sanction disciplinaire

1.3.3 Stratégie de traitement

Pour chaque événement redouté, l'arbitrage Direction/RSSI conduit à l'une des quatre stratégies suivantes : éviter, réduire, transférer (assurance cyber) ou accepter de manière documentée. À ce

jour, l'approche retenue est très majoritairement la réduction du risque par des mesures techniques et organisationnelles décrites au chapitre 4. Aucun risque résiduel n'est accepté sans visa explicite et daté du Directeur Général.

2. Gouvernance et pilotage de la sécurité

2.1 Principes directeurs de la gouvernance

La gouvernance de la sécurité de l'information de BIOÉNERGIE TECH repose sur trois principes intangibles : (i) un portage direct par la Direction Générale, qui demeure responsable juridique ; (ii) une séparation claire des fonctions d'exploitation et de contrôle ; (iii) une démarche d'amélioration continue alignée sur le cycle PDCA (Plan – Do – Check – Act) issu de l'ISO/IEC 27001.

2.2 Rôles, instances et responsabilités

Rôle / Instance	Missions principales	Périodicité d'intervention
Direction Générale (DG)	Valide la PSSI et ses évolutions ; arbitre les risques résiduels ; alloue le budget sécurité ; nomme le RSSI ; assume la responsabilité juridique au titre de l'IGI 1300 et de NIS 2.	Annuelle + ad-hoc en cas d'incident majeur
Responsable de la Sécurité des SI (RSSI)	Élabore et maintient la PSSI ; pilote l'analyse de risques EBIOS RM ; orchestre la gestion des incidents ; tient les indicateurs ; représente l'entreprise auprès de l'ANSSI et de l'autorité de sécurité espagnole.	Permanente
Administrateur du SI cloisonné	Met en œuvre les mesures techniques prescrites : Active Directory, PKI interne, configuration du pare-feu Cisco 1120 et du switch Cisco 9200, ELK, sauvegardes LTO, station blanche, comptes à privilèges.	Permanente
Comité de Sécurité (COSEC)	Présidé par le DG, associe RSSI,, administrateur, responsable projet SpainTurbine, responsable RH. Revoit les indicateurs, valide le plan d'action, suit les RETEX d'incidents.	Trimestrielle
Cellule de Crise Cyber	Activée par le RSSI sur déclenchement d'un incident majeur. Inclut DG, RSSI, administrateur, responsable juridique, communication, et le cas échéant le prestataire d'investigation.	À l'activation
Référents sécurité projet	Chacun des 5 salariés habilités SpainTurbine relaie les consignes, signale les événements suspects, et participe aux exercices de sensibilisation.	Continue
Auditeur externe / organisme de certification	Conduit les audits indépendants ; ses accès sont supervisés par l'administrateur (cf. matrice d'accès externes du DAT).	Annuelle

2.3 Documentation et corpus normatif interne

La PSSI constitue le document de niveau 1. Sont articulés en dessous : (a) les politiques spécifiques (politique d'authentification, politique de sauvegarde, politique de gestion des incidents) ; (b) les procédures opérationnelles (PO-IAM, PO-SAUV-LTO, PO-STATION-BLANCHE) ; (c) les modes opératoires détaillés ; (d) les chartes utilisateur signées individuellement. Tout document doit obligatoirement comporter une référence, un visa du RSSI, une date d'application et une période de revue.

2.4 Sanctions et régime disciplinaire

Tout manquement aux dispositions de la PSSI fait l'objet d'une instruction par le RSSI, puis d'une décision proportionnée prise par la Direction Générale après avis du COSEC. Les sanctions vont de l'avertissement écrit au licenciement pour faute grave, sans préjudice des poursuites pénales lorsque la violation porte atteinte au secret de la défense nationale (articles 413-9 et suivants du Code pénal). Tout contrat de sous-traitance comporte une clause miroir de la présente PSSI assortie de pénalités contractuelles.

3. Gestion des accès (IAM) et traçabilité

3.1 Principes directeurs de l'IAM

La gestion des identités et des accès du SI cloisonné s'appuie sur six principes opposables : (i) le « besoin d'en connaître » et le moindre privilège ; (ii) la séparation des rôles entre exploitation, administration et audit ; (iii) l'authentification forte multi-facteurs pour tout accès logique ; (iv) la traçabilité exhaustive et non répudiable de chaque action ; (v) la revue périodique des droits ; (vi) la révocation immédiate sur événement RH.

3.2 Classification des données et niveaux d'habilitation

Quatre niveaux de classification sont définis et opposables :

Niveau	Définition	Stockage / Transport	Exemples
Confidencial (C4)	Information dont la divulgation porterait une atteinte grave à la sécurité de l'État espagnol ou à la défense	Chiffrement systématique, PC chiffrement dédié, transport en valise scellée sous deux signatures	Plans micro-turbines, paramètres machines, présérie
Sensible (C3)	Information stratégique BIOÉNERGIE TECH	Serveur de fichiers cloisonné, SMB v3 chiffré, ACL AD strictes	Journaux ELK, vidéo Axis, données RH
Interne (C2)	Information à usage interne	Stockage standard avec authentification	Documentation procédures, modes opératoires
Public (C1)	Information diffusable	Stockage non restreint	Plaquette commerciale, communiqués

À chaque niveau de classification correspond une habilitation nominative. Aucun salarié, aucun sous-traitant et aucun visiteur ne peut accéder à une information classifiée « Confidencial » sans habilitation préalable validée par la Direction Générale et, le cas échéant, par l'autorité de sécurité espagnole compétente.

3.3 Matrice d'accès – Personnel interne

La matrice ci-après prolonge celle inscrite au DAT et précise les méthodes d'authentification opposables :

Entité	Droits et privilèges	Méthode d'authentification	Niveau habilitation
PDG	Accès aux locaux uniquement	Badge nominatif	Confidencial
5 salariés du projet SpainTurbine	Accès aux locaux, PC employés, serveur de fichiers (besoin d'en connaître)	Badge + YubiKey C NFC sur PC + biométrie SAS	Confidencial
Administrateur SI	Accès locaux, salle serveur, serveurs, équipements réseau, ELK, PKI	Badge + YubiKey C NFC + biométrie SAS + comptes à privilèges nominatifs	Confidencial

Employés hors projet	Aucun accès à la zone classifiée	Aucun moyen d'authentification provisionné	—

3.4 Matrice d'accès – Intervenants externes

Entité externe	Droits et conditions d'accès	Méthode d'authentification	Supervision
Femme/Homme de ménage	Aucun accès à la zone classifiée	—	—
Fournisseur télécom	Accès uniquement en période de travaux à titre exceptionnel	Badge journalier nominatif	Supervision continue par l'administrateur
Organisme de certification / audit	Accès aux locaux et, séparément, aux serveurs sur autorisation écrite préalable	Badge journalier nominatif	Locaux : employé projet ou PDG / Serveurs : administrateur
Sous-traitant matériel (station blanche, etc.)	Accès aux locaux uniquement pour intervention planifiée	Badge journalier nominatif	Supervision continue par employé projet ou PDG
Visiteurs	Sans accès aux zones classifiées	Inscription au registre, accompagnement permanent	Permanente

3.5 Cycle de vie des identités

Le cycle de vie est piloté conjointement par les RH et le RSSI selon le processus suivant, opposable et journalisé dans ELK :

- **Arrivée :** instruction d'habilitation, signature de la charte sécurité et de la clause de confidentialité défense, formation initiale obligatoire, remise du badge nominatif et de la YubiKey, création des comptes Active Directory avec MFA, attribution des ACL « besoin d'en connaître ».
- **Mobilité :** revue exhaustive des droits sous 48 h, révocation des droits non justifiés, ré-instruction d'habilitation si changement de périmètre de classification.
- **Départ :** révocation immédiate des badges et YubiKey, désactivation des comptes AD avant la fin de la dernière journée travaillée, rappel écrit de l'obligation de confidentialité post-emploi, archivage des journaux pendant 36 mois.
- **Revue périodique :** revue trimestrielle des comptes par l'administrateur et le RSSI ; tout compte inutilisé depuis plus de 60 jours est désactivé automatiquement ; tout compte à privilèges est revu mensuellement.

3.6 Authentification, chiffrement et secrets

L'authentification s'appuie sur les technologies retenues au DAT et complétées par les règles suivantes :

- **MFA obligatoire :** badge nominatif + YubiKey C NFC FIDO U2F/FIDO2 pour tout accès logique aux PC employés et au PC de chiffrement ; ajout d'un facteur biométrique HID Signo 25B pour franchir le SAS d'accès puis le local sécurité.
- **Kerberos et LDAPS :** authentification au domaine Active Directory chiffrée TLS, renouvellement des tickets selon la politique du domaine, comptes Kerberos AES-256.
- **PKI interne :** émission, distribution et révocation des certificats pour authentification machines, signature des journaux et chiffrement SMB v3 ; publication régulière de la CRL.
- **Chiffrement des supports :** disques internes des PC et serveurs chiffrés intégralement (BitLocker entreprise ou équivalent) ; bandes LTO-8 chiffrées matériellement par le lecteur HPE Ultrium 30750 ; clés stockées dans le coffre-fort à six compartiments à serrures à code distinctes par administrateur.
- **Comptes à privilèges :** comptes nominatifs distincts du compte utilisateur courant ; obligation d'un compte par administrateur ; aucun compte « root » ou « administrator » partagé ; mots de passe administrateurs >= 16 caractères, changement obligatoire tous les 90 jours, jamais ré-utilisés.
- **YubiKey de secours :** sur les 5 YubiKey C NFC du parc, une clé est conservée scellée dans le coffre-fort comme moyen de recouvrement de dernier ressort accessible uniquement sur signature du DG et du RSSI.

3.7 Traçabilité et imputabilité

Toute action significative est tracée, horodatée et signée. Les exigences minimales sont :

- Collecte centralisée dans ELK (Elasticsearch / Logstash / Kibana) des journaux Windows, serveurs, Active Directory, PKI, switch Cisco Catalyst 9200, lecteurs biométriques et flux vidéo Axis M4216-V (métadonnées).
- Synchronisation NTP commune sur l'ensemble du SI cloisonné, vérifiée mensuellement par l'administrateur.
- Conservation des journaux pendant 36 mois (12 mois en ligne dans ELK + 24 mois sur bande LTO en coffre-fort).
- Intégrité des journaux garantie par signature et indexation horodatée ; toute tentative de modification déclenche une alerte Kibana.
- Tableaux de bord Kibana dédiés au RSSI : accès privilégiés, événements de sécurité, échecs d'authentification, alertes EDR, mouvements de bandes LTO.
- Revue hebdomadaire des alertes par l'administrateur, revue mensuelle des indicateurs par le RSSI, revue trimestrielle par le COSEC.

4. Règles d'utilisation et dispositifs de protection (sécurité opérationnelle)

4.1 Règles d'utilisation du système d'information

Les règles suivantes sont opposables à tout utilisateur de la zone classifiée. Elles sont consignées dans la charte sécurité annexée au contrat de travail et au contrat de sous-traitance.

4.1.1 Règles applicables aux utilisateurs

- Il est obligatoire de verrouiller la session (touche Windows + L) à chaque départ du poste, même pour une absence brève, et de ranger systématiquement YubiKey et documents sensibles dans le tiroir sécurisé.
- Il est obligatoire de signaler sans délai au RSSI tout événement suspect : email douteux, comportement anormal d'un poste, perte de YubiKey ou de badge, accès non sollicité d'un tiers, support amovible inconnu trouvé sur site.
- Il est interdit de connecter un support amovible personnel (clé USB, disque externe, téléphone) sur les postes opérationnels ou la salle serveur. Tout support entrant doit obligatoirement transiter par la station blanche S3Box Hogo.
- Il est interdit d'utiliser un service de messagerie ou un service cloud personnel pour traiter ou transmettre des données classifiées.
- Il est interdit de photographier les écrans, les équipements ou les documents classifiés, sauf autorisation expresse du RSSI.
- Il est interdit d'introduire ou de sortir tout document papier classifié sans inscription au registre de mouvements documentaires et signature du PDG.
- Il est interdit d'installer ou d'exécuter tout logiciel non figurant à la liste blanche maintenue par l'administrateur.
- Il est obligatoire de respecter le principe du « bureau propre / écran propre » en fin de journée et en cas d'absence prolongée.

4.1.2 Règles applicables aux administrateurs

- Les administrateurs doivent utiliser exclusivement leurs comptes nominatifs à privilèges, jamais leurs comptes utilisateurs courants pour des tâches d'exploitation.
- Les administrateurs doivent documenter dans l'outil de tickets toute intervention sur le SI cloisonné, avec horodatage, justification et résultat.
- Les administrateurs doivent appliquer le principe « quatre yeux » pour toute action irréversible critique (suppression de comptes à privilèges, modification de l'ACL racine, restauration depuis bande LTO, désactivation d'un mécanisme de sécurité).
- Les administrateurs doivent appliquer les correctifs de sécurité dans les délais ANSSI : sous 72 h pour les vulnérabilités critiques, sous 30 jours pour les autres,4.1.3 Règles applicables aux tiers
- Les tiers (auditeurs, fournisseur télécom, sous-traitants matériels) ne disposent jamais d'accès permanent. Tout accès est nominatif, daté, supervisé en présence d'un employé projet ou de l'administrateur, et journalisé.
- Les contrats de sous-traitance comportent une clause miroir de la présente PSSI, une obligation de notification d'incident dans les 24 h, et un droit d'audit BIOÉNERGIE TECH.

4.2 Dispositifs concrets de protection issus du DAT

Aux règles ci-dessus correspondent des dispositifs techniques précis, déjà inventoriés dans le DAT de BIOÉNERGIE TECH. Chaque dispositif est associé à un responsable, à une fréquence de contrôle et à un indicateur de sécurité (cf. chapitre 8).

Catégorie	Dispositif retenu (DAT)	Fonction de sécurité
Périmètre physique	SAS d'accès avec lecteurs biométriques HID Signo 25B (×2) et caméra IP Axis M4216-V	Contrôle physique des accès, surveillance, traçabilité visuelle
Périmètre physique	Coffre-fort Fichet-Bauche Carena 120 L + coffre à 6 compartiments cloisonnés	Mise en sécurité des bandes LTO et des secrets cryptographiques
Périmètre physique	Verrous physiques USB (×30) et verrous RJ45 (×20)	Prévention de connexion non autorisée de supports ou de câbles
Réseau	Switch Cisco Catalyst 9200 avec VLAN cloisonnés et ACL strictes	Segmentation interne, contrôle de propagation latérale
Réseau	Pare-feu Cisco Secure Firewall 1120	Filtrage des rares flux autorisés, journalisation, blocage des flux non explicitement autorisés (deny by default)
Postes / serveurs	3 PC HP Elite 800 G9 employés, 1 PC mise à jour, 1 PC chiffrement, 2 serveurs Dell PowerEdge R470	Cloisonnement des usages (production / maintenance / chiffrement), redondance serveur
Endpoint	EDR à déployer sur les 5 PC et 2 serveurs (signatures + comportemental)	Détection et confinement des menaces sur poste
Sas amovible	Station blanche S3Box Hogo	Analyse anti-malware multi-moteurs de tout support amovible avant introduction
Authentification	5 YubiKey C NFC FIDO U2F/FIDO2	Authentification forte non phishable
Identité	Active Directory + PKI interne + Kerberos / LDAPS	Gestion centralisée des comptes, certificats, chiffrement des flux
Journalisation	Pile ELK (Elasticsearch, Logstash, Kibana)	Centralisation, corrélation et restitution des journaux
Sauvegarde	Lecteur HPE StoreEver LTO-8 Ultrium 30750 + 15 cartouches LTO-8	Sauvegarde hors-ligne chiffrée, opposable au rançongiciel
Médias chiffrés	PC dédié chiffrement/déchiffrement	Préparation des supports sortants chiffrés vers SpainTurbine

4.3 Sécurité physique et environnementale

Au-delà des dispositifs ci-dessus, le périmètre physique doit faire l'objet des mesures suivantes, justifiées par la coactivité industrielle et la proximité d'installations Seveso (CHEMICALIA à 40 m, métallurgistes à 80–100 m, voie ferrée fret < 200 m, Rhône à 1–2 km) :

- Détection incendie multi-points avec extinction adaptée à la salle serveur (gaz inerte), test semestriel.
- Onduleur dimensionné pour 30 min d'autonomie, groupe électrogène mutualisé avec le bâtiment principal, test mensuel à charge.
- Surveillance vidéo H.264/RTSP de la zone d'accès (caméra Axis M4216-V) en VLAN isolé, enregistrement 30 jours.
- Plan de prévention CHSCT/CSE intégrant le risque chimique voisin et organisant l'évacuation contrôlée du SI sensible.
- Marquage des câbles, fixation des panneaux et inspection trimestrielle des dispositifs anti-vibrations.

5. Protection des données, localisation et risques tiers

5.1 Doctrine de localisation : interdiction de l'externalisation cloud

La doctrine retenue par BIOÉNERGIE TECH pour la zone Confidencial est claire et opposable : toute donnée classifiée « Confidencial » est strictement maintenue dans le périmètre physique du site de Chambéry. Il est interdit d'utiliser tout service de cloud public ou privé hébergé hors du périmètre maîtrisé. Cette interdiction couvre notamment : SaaS bureautiques, messageries grand public, services de partage de fichiers, services de visioconférence non maîtrisés, sauvegarde cloud, et tout service d'hébergement étranger.

5.2 Cycle de vie des données classifiées

Étape	Mesure prescrite	Dispositif support
Création	Marquage automatique « Confidencial » des documents par modèle Office centralisé ; refus de création hors postes opérationnels	Postes HP Elite 800 G9, ACL Active Directory
Stockage	Stockage exclusif sur serveur de fichiers du SI cloisonné, ACL par groupe AD avec besoin d'en connaître	SMB v3 chiffré, PowerEdge R470, chiffrement disque
Transport interne	Aucun support amovible non chiffré ; analyse systématique en station blanche pour tout support entrant	Station blanche S3Box Hogo
Transport externe	Chiffrement systématique sur le PC dédié chiffrement, support en valise scellée à double signature, registre de mouvement	PC chiffrement, coffre à 6 compartiments
Sauvegarde	Chiffrement matériel LTO-8 ; rotation des bandes selon calendrier ; dépôt hebdomadaire en coffre-fort	Lecteur HPE StoreEver, cartouches IBM LTO-8, coffre Fichet-Bauche Carena
Archivage	Conservation des données 10 ans pour les éléments contractuels, 36 mois pour les journaux, dans le coffre-fort dédié	Coffre-fort
Destruction	Effacement cryptographique par destruction de la clé puis destruction physique des supports (broyage), procès-verbal contresigné DG + RSSI	Prestataire qualifié sur site

5.3 Maîtrise des risques tiers et chaîne d'approvisionnement

La présence permanente ou ponctuelle d'intervenants tiers (fournisseur télécom, sous-traitant station blanche, organisme d'audit, personnels de ménage, etc.) constitue l'un des principaux scénarios de compromission identifiés (cf. § 1.3). Les mesures suivantes s'appliquent :

- **Sélection :** évaluation préalable du prestataire (financière, juridique, sécurité), prise en compte de la nationalité du capital, exigence d'une certification ISO/IEC 27001 ou équivalente lorsque le prestataire traite des données sensibles.
- **Contractualisation :** clause de confidentialité défense, clause miroir PSSI, droit d'audit, obligation de notification d'incident sous 24 h, sous-traitance en cascade soumise à autorisation écrite.
- **Habilitation et accès :** badge journalier nominatif, accompagnement permanent par un employé projet ou par l'administrateur, plage horaire imposée, journalisation dans ELK et inscription au registre des accès.
- **Supervision :** toute intervention sur la salle serveur ou sur la station blanche fait l'objet d'un compte-rendu signé par l'administrateur ; toute modification de configuration est rejouée en revue par le RSSI.
- **Sortie de prestation :** révocation immédiate des badges, restitution des documents, rappel des obligations post-contractuelles, vérification des journaux d'accès et conservation pendant 36 mois.

5.4 Conformité RGPD pour les données personnelles

Les données à caractère personnel des 5 salariés habilités, ainsi que celles des prestataires (état civil, badge, biométrie, contrôles d'accès, vidéo), font l'objet d'un registre des traitements tenu par le DPO. Une analyse d'impact (PIA) est conduite pour le traitement biométrique HID Signo 25B et la vidéosurveillance Axis M4216-V. Les durées de conservation sont strictement limitées : 30 jours pour la vidéo, 36 mois pour les journaux d'accès, durée du contrat + 24 mois pour les habilitations. Les personnes concernées sont informées et leurs droits sont exerçables auprès du DPO.

6. Gestion des incidents de sécurité et amélioration continue

6.1 Cycle de vie des incidents – traduction textuelle du processus interne

BIOÉNERGIE TECH applique le processus de gestion des incidents formalisé dans son support cartographique interne (« processus_gestion_incidents.drawio »). Ce processus est opposable et constitue la traduction opérationnelle des principes ISO/IEC 27035 et du Guide ANSSI « Réagir à une attaque informatique ». Il s'articule en trois phases successives : Préparation, Détection, Traitement (système ou adversaire), suivies d'un retour à la phase Préparation après chaque incident.

6.1.1 Phase de préparation

La phase de préparation, antérieure à tout événement, comprend trois activités permanentes :

- **Gouverner :** publication et maintien de la présente PSSI, allocation budgétaire, désignation des rôles, exercices de crise.
- **Identifier :** cartographie des actifs primordiaux (cf. § 1.2), maintien du DAT à jour, analyse de risques EBIOS RM, veille sur les vulnérabilités CVE et les indicateurs de compromission.
- **Protéger :** déploiement et durcissement des dispositifs techniques (pare-feu, EDR, station blanche, ELK, sauvegardes LTO), sensibilisation continue des 5 salariés habilités, exercices de simulation phishing.

6.1.2 Phase de détection et de qualification

La phase de détection repose sur la centralisation des journaux dans ELK et sur la remontée d'alertes par les utilisateurs. Tout événement est qualifié, dès son apparition, par l'administrateur, qui répond à la question : « S'agit-il d'un événement système normal (mise à jour planifiée, stockage, redémarrage…) ? »

- **Si OUI – événement normal :** retour direct à la phase de Préparation, après inscription au journal de bord opérationnel.
- **Si NON – événement anormal :** qualification en « Événement Système » ou en « Événement Adversaire » selon la nature observée et déclenchement de la phase de traitement correspondante.

6.1.3 Phase de traitement – Événements Système

Trois sous-catégories d'événements système sont traitées :

- **Défaillance système (System failure) :** alerte immédiate de l'équipe infrastructure, bascule sur le serveur de redondance PowerEdge R470, ouverture d'un ticket d'incident et investigation des causes racines.
- **Dommage physique (Physical damages) :** alerte immédiate de l'équipe infrastructure et activation du PCA matériel (cf. chapitre 7), constat photographique, dépôt de main courante si origine externe.
- Divulgation accidentelle (Accidental disclosure) – arborescence de décision :
    - **Téléchargement accidentel de données critiques :** identifier sur quelle plateforme la donnée a été téléchargée, puis vérifier la possibilité de suppression directe.
    - → **Si suppression possible :** supprimer immédiatement la donnée et notifier l'utilisateur fautif.

- → **Si suppression impossible :** empêcher l'administrateur de la plateforme tierce de supprimer pour préserver les traces, et notifier l'utilisateur fautif. Sanction proportionnée appliquée au titre du § 2.4.
- **Courriel accidentel contenant des informations sensibles :** supprimer le courriel (rappel et purge boîte destinataire si possible) et notifier l'utilisateur fautif.

6.1.4 Phase de traitement – Événements Adversaires

Lorsqu'un événement adversaire est détecté (accès aux données clients, disruption de services, vol d'informations stratégiques, sabotage interne), le RSSI active la cellule de crise et entre dans l'arbre de décision « Identifier l'attaque ». Sept catégories d'attaques sont prises en charge ; à chacune correspond un enchaînement de mesures opérationnelles :

Type d'attaque	Arbre de décision (traduit textuellement du processus interne)
Exploitation de vulnérabilité	Est-ce une vulnérabilité distante ? Oui → bloquer l'IP source au pare-feu Cisco 1120, isoler la machine, appliquer le correctif et tester. Non → isoler la machine, appliquer le correctif, tester. Objectif final : empêcher l'exploitation côté client.
Attaque par force brute	Bloquer l'IP source au pare-feu Cisco 1120, durcir la politique de mots de passe et le verrouillage de compte AD, empêcher la poursuite côté client.
Élévation de privilèges	S'agit-il d'un compte local ? Oui → isoler la machine concernée. Non → bloquer le compte AD ciblé. Dans les deux cas, prévenir le service RH afin de tracer la responsabilité et déclencher une instruction disciplinaire si nécessaire.
Altération de la configuration système	L'altération modifie-t-elle l'accès distant ? Oui → bloquer immédiatement l'IP à l'origine de la modification, restaurer la configuration antérieure depuis la dernière sauvegarde validée, tester le retour à la normale. Désactive-t-elle un mécanisme de sécurité ? Oui → restaurer la configuration. Modifie-t-elle le système de sauvegarde ? Oui → restaurer la configuration. Dans tous les cas : tester la remise en service.
Logiciel malveillant	Identifier les actifs affectés, qualifier le type de malware, isoler les machines infectées du réseau, créer une image disque (forensique) des systèmes compromis, préparer la sauvegarde, restaurer les systèmes, puis ouvrir une investigation détaillée.
Hameçonnage (phishing)	L'email contient-il une URL ou une pièce jointe ? Pièce jointe : calculer le hash, analyser sur VirusTotal puis avec les règles YARA, bloquer l'IP de l'expéditeur sur le pare-feu, supprimer le courriel. URL : analyser sur VirusTotal, bloquer l'IP, supprimer le courriel. Dans les deux cas : notifier l'utilisateur ciblé.
Déni de service (DoS / DDoS)	Mettre en œuvre un équilibrage de charge le cas échéant, arrêter les services ciblés pour limiter l'impact, bloquer le trafic d'attaque sur le pare-feu Cisco 1120, puis redémarrer les services concernés.

6.2 Notification et communication des incidents

Toute violation avérée ou suspectée de la confidentialité d'une donnée classifiée « Confidencial » est notifiée par le RSSI :

- Sans délai à la Direction Générale et à la cellule de crise.
- Sous 24 h au point de contact contractuel de SpainTurbine et à l'autorité de sécurité espagnole compétente, conformément à la clause défense du contrat.
- Sous 24 h à l'ANSSI au titre de NIS 2, et sous 72 h à la CNIL en cas de violation de données à caractère personnel relevant du RGPD.

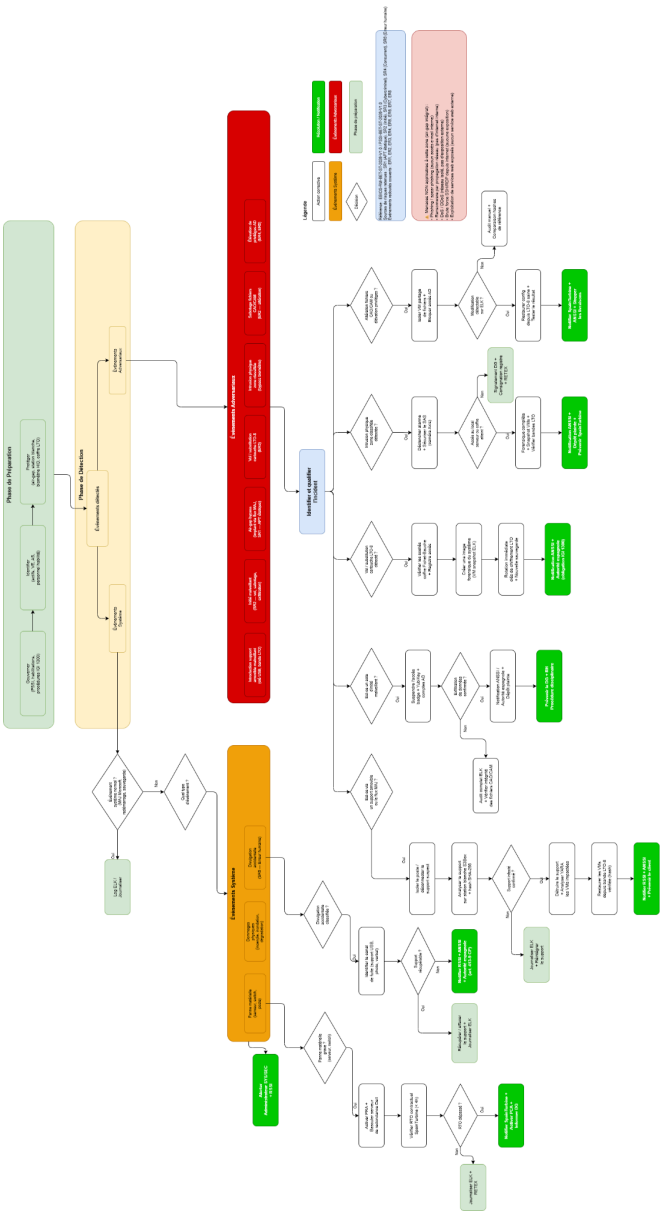
- Aux autorités judiciaires en cas de présomption d'atteinte au secret de la défense nationale (art. 413-9 et suivants du Code pénal).

6.3 Retour d'expérience et amélioration continue

Chaque incident, qu'il soit système ou adversaire, fait l'objet d'un RETEX écrit clôturant le ticket, contresigné par l'administrateur et le RSSI. Le RETEX est revu en COSEC trimestriel et alimente :

- Une mise à jour ciblée du DAT et de la présente PSSI (révision dirigée).
- Une révision des règles de détection ELK (création de nouveaux dashboards Kibana, ajustement des seuils d'alerte, ajout de nouvelles requêtes Logstash).
- Une révision des procédures opérationnelles, des chartes utilisateurs et des supports de sensibilisation.
- Un plan d'action pluriannuel piloté par le RSSI, intégrant les recommandations d'audit interne et externe (audit annuel obligatoire).
- Une revue annuelle de l'analyse de risques EBIOS RM pour ajuster la liste des sources de risque, des scénarios stratégiques et des scénarios opérationnels.

Diagramme de la gestion des incidents :



7. Continuité d'activité et résilience (PCA / PRA)

7.1 Objectifs de continuité

Les engagements contractuels pris envers SpainTurbine (120 micro-turbines mensuelles) imposent une continuité maîtrisée de la chaîne de production assistée. Les objectifs suivants sont opposables :

Indicateur	Cible	Justification
RTO (durée maximale d'interruption admissible)	≤ 4 heures pour les services critiques (AD, fichiers, ELK)	Maintien de la production journalière
RPO (perte maximale de données admissible)	≤ 24 heures (sauvegarde incrémentale quotidienne LTO-8)	Aligne RPO et politique de sauvegarde DAT
MTPD (durée maximale tolérable de perturbation)	≤ 72 heures	Au-delà : pénalités contractuelles, risque de rupture

7.2 Stratégie de sauvegarde et de restauration

La stratégie de sauvegarde et de restauration reprend et formalise la doctrine inscrite au DAT :

- **Infrastructure :** un serveur principal et un serveur de redondance Dell PowerEdge R470 ; bascule à chaud sur le serveur redondant en cas de défaillance.
- **Média :** bandes magnétiques LTO-8 (15 cartouches IBM Ultrium 8) lues/écrites par le lecteur HPE StoreEver Ultrium 30750, chiffrement matériel activé.
- **Fréquence :** sauvegarde complète hebdomadaire le vendredi soir hors heures ouvrées, sauvegarde incrémentale quotidienne en fin de journée.
- **Rotation :** modèle « grand-père / père / fils » sur 4 semaines, avec quatre cartouches conservées hors site (dans une zone sécurisée dans le premier site..).
- **Stockage :** dépôt hebdomadaire des bandes dans le coffre-fort Fichet-Bauche Carena 120 L, registre nominatif des mouvements de bandes.
- **Test de restauration :** test mensuel de restauration partielle ; test annuel de restauration complète sur le serveur de redondance, procès-verbal contresigné DG + RSSI.
- **Air-gap :** les bandes ne sont jamais connectées simultanément à plusieurs systèmes ; le lecteur LTO est branché à la demande, supervisé par l'administrateur.

7.3 Plan de Continuité (PCA) et Plan de Reprise (PRA)

Le PCA garantit la poursuite des activités sensibles malgré une perturbation ; le PRA encadre la reprise après sinistre majeur. Ils s'articulent selon les scénarios suivants :

Scénario	Conséquence redoutée	Stratégie de continuité
Défaillance serveur principal	Indisponibilité Active Directory, partages SMB v3, PKI	Bascule serveur de redondance PowerEdge R470 (RTO ≤ 1 h)
Compromission rançongiciel du SI cloisonné	Chiffrement des données serveurs et postes	Isolation immédiate, restauration depuis bandes LTO en coffre, repavage des postes (RTO ≤ 4 h)

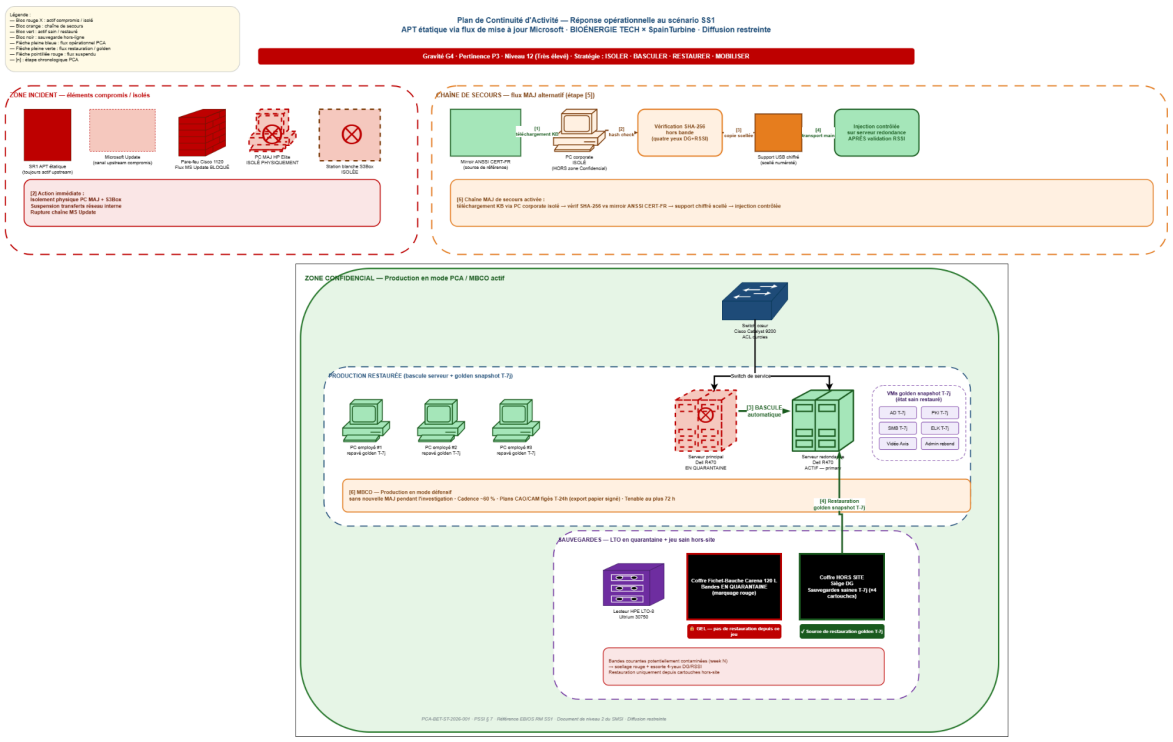
Sinistre majeur sur site (incendie/inondation/CHEMICALIA)	Destruction physique du local sécurité	Réplication contractuelle des bandes hors site (dans une zone sécurisée dans le premier site), site de secours sur le bâtiment principal, marché-cadre PRA avec intégrateur qualifié (RTO ≤ 72 h)
Indisponibilité prolongée d'un salarié habilité	Concentration des habilitations sur 5 personnes	Polyvalence documentée des 5 habilités, plan de remplacement, dossier d'habilitation préparé pour 1 réserviste
Coupure électrique générale	Arrêt des serveurs et équipements réseau	Onduleur 30 min + groupe électrogène mutualisé
Coupure télécom prolongée	Pas de mises à jour	Isolation déjà acquise (air-gap), pas d'impact opérationnel direct ; mise à jour différée

7.4 Exercices de continuité

Un exercice de continuité est conduit chaque année selon un scénario tiré au sort parmi ceux du § 7.3. Un exercice de crise cyber « tabletop » est conduit chaque semestre. Les RETEX sont consignés et alimentent la PSSI ainsi que les procédures opérationnelles.

Schéma du Plan de Continuité d’activité - Réponse opérationnelle au scénario SS1.

APT étatique via flux de mise à jour Microsoft . BIOENERGIE TECH x Spain Turbine . Diffusion restreinte


Légende
— Bloc rouge V. : actif compromis / isolé
— Bloc orange : chaîne de secours
— Bloc vert : actif sain / restauré
— Bloc noir : sauvegarde hors-ligne
— Flèche pleine bleue : flux opérationnel PCA
— Flèche pleine verte : flux restauration / golden
— Flèche pointillée rouge : PC Incidents
— P1 : étape chronologique PCA
Plan de Continuité d'Activité — Réponse opérationnelle au scénario S1
APT étatique via flux de mise à jour Microsoft · BIOÉNERGIE TECH × SpainTurbine · Diffusion restreinte
Gravité G4 · Pertinence P3 · Niveau 12 (Très élevé) · Stratégie : ISOLER · BASCULER · RESTAURER · MOBILISER
ZONE INCIDENT — éléments compromis / isolés
SRV1-APT étatique
Microsoft Update
Pare-feu Cisco 1120
PC MAJ HP Elite
Station blanche S3Box
[2] Action immédiate :
Isolement physique PC MAJ + S3Box
Suspension transferts réseau interne
Rupture chaîne MS Update
CHAÎNE DE SECOURS — flux MAJ alternatif (étape [5])
Mirror ANSSI CERT-FR
PC corporate
Vérification SHA-256
Support USB chiffré
Injection contrôlée
[5] Chaîne MAJ de secours activée :
ZONE CONFIDENTIEL — Production en mode PCA / MBCO actif
Switch de service
PRODUCTION RESTAURÉE (bascule serveur + golden snapshot T-7j)
PC employé #1
PC employé #2
PC employé #3
Serveur principal
Serveur redondant
[3] BASCULE automatique
Vm golden snapshot T-7j
(état sain restauré)
AD T-7j
PKI T-7j
SMB T-7j
ELK T-7j
Vielle Axia
Admin rebond
[6] MBCO — Production en mode dégradé
sans nouvelle MAJ pendant l'investigation · Cadence −60 % · Plans CAO/CAM figés T-24h (export papier signé) · Tenable au plus 72 h
[4] Restauration
golden snapshot T-7j
SAUVEGARDES — LTO en quarantaine + jeu sain hors-site
Lecteur HPE LTO-9
Ultrium 30750
Coffre Fichet Guardia Caseau 120 L
Rendre EN QUARANTAINE
(marquage rouge)
Coffre HORS SITE
Siège DG
Sauvegardes saines T-7j (X4
cartouches)
Bandes courantes potentiellement contaminées (week-to)
— scellage rouge + cassette 4 yeux DG/RSSI
Restauration uniquement depuis cartouches hors-site
PCA-BET-ST-2026-001 · PSSI §.7 · Référence EBIOS RM SS1 · Document de niveau 2 du SMSI · Diffusion restreinte

8. Conformité, mesure et arbitrage stratégique

8.1 Conformité réglementaire et normative

La conformité est assurée par un référencement explicite de chaque exigence de la présente PSSI à un article de norme ou de réglementation, consigné dans une matrice de conformité tenue par le RSSI.

Référentiel	Articles / chapitres clés mobilisés	Mesures BIOÉNERGIE TECH
RGPD (UE 2016/679) et Loi Informatique & Libertés	Art. 5, 25, 32, 33, 35	Registre des traitements (DPO), PIA biométrie HID Signo 25B et vidéo Axis, durées de conservation, notification de violation < 72 h
Directive NIS 2 (UE 2022/2555)	Art. 20, 21, 23	Mesures techniques (4.2), gouvernance (chap. 2), gestion des incidents (chap. 6), notification ANSSI
IGI 1300 / cadre Confidencial espagnol	Tous chapitres	Cloisonnement physique et logique, habilitations nominatives, chiffrement, traçabilité
ISO/IEC 27001:2022	Annexe A complète	Gouvernance (chap. 2), IAM (chap. 3), opérations (chap. 4), incidents (chap. 6), continuité (chap. 7)
ISO/IEC 27002:2022	Mesures organisationnelles, techniques, physiques, humaines	Politiques, charte sécurité, sensibilisation, contrôles physiques
ISO/IEC 27035:2023	Gestion des incidents	Processus interne de gestion des incidents (chap. 6)
ANSSI – EBIOS RM v1.5	5 ateliers	Analyse de risques (chap. 1)
Code pénal	Art. 413-9 et s.	Sanctions, clauses contractuelles, notifications judiciaires

8.2 Indicateurs et tableaux de bord (KPI / KRI)

Le RSSI tient un tableau de bord sécurité restitué mensuellement à la Direction Générale et trimestriellement au COSEC. Les indicateurs minimaux sont :

Indicateur	Définition	Cible	Fréquence
Taux d'application des correctifs critiques sous 72 h	Correctifs critiques appliqués dans les délais / total	≥ 95 %	Mensuelle
Taux de couverture EDR sur les 5 PC et 2 serveurs	Machines avec EDR à jour / parc total	100 %	Mensuelle
Nombre d'incidents détectés / qualifiés / clôturés	Nombre par mois	Suivi tendance	Mensuelle
Temps moyen de détection (MTTD)	Entre apparition et alerte qualifiée	≤ 24 h	Trimestrielle

Temps moyen de réponse (MTTR)	Entre alerte qualifiée et clôture	≤ 48 h pour les majeurs	Trimestrielle
Taux de réussite des tests de restauration	Restaurations validées / tentatives	100 %	Mensuelle
Taux de comptes inactifs > 60 j	Comptes inactifs / total	0 %	Mensuelle
Taux de salariés sensibilisés dans l'année	Salariés ayant suivi la formation / habilités	100 %	Annuelle
Taux de clics sur exercices phishing	Clics / envois	≤ 5 %	Semestrielle
Nombre de RETEX clos	RETEX clos / incidents	100 % à 90 j	Trimestrielle
Nombre d'audits internes/externes réalisés	Audits réalisés / planifiés	100 %	Annuelle
Couverture de la matrice de conformité	Exigences couvertes / total	≥ 95 %	Annuelle

8.3 Arbitrage : sécurité, continuité, performance, budget

Le caractère de PME (49 collaborateurs, dont 5 dédiés au projet SpainTurbine) et le budget effectivement engagé sur les équipements de sécurité (109 400,35 € HT, soit ~9 % du chiffre d'affaires annuel du contrat) imposent un arbitrage permanent. La doctrine retenue par BIOÉNERGIE TECH est résumée comme suit :

Exigence	Tension identifiée	Arbitrage retenu et justification
Sécurité maximale vs. coût	Investissement initial > 100 k€ et coûts récurrents (sensibilisation, audit, restauration)	Investissement assumé sur 3 ans, amortissement aligné sur la durée du contrat ; aucune zone grise sur la chaîne d'approvisionnement défense
Cloisonnement strict (air-gap) vs. productivité	Mises à jour, échanges documentaires et audits ralentis par le filtre station blanche	Maintien de l'air-gap (non négociable au regard du Confidencial) ; optimisation du poste mise à jour et de la station blanche pour réduire les temps de cycle
Sauvegarde hors-ligne LTO vs. immédiateté de restauration	RTO supérieur à une sauvegarde en ligne	Compromis assumé : LTO offre la meilleure protection contre le rançongiciel ; bascule serveur redondant pour les services critiques (RTO ≤ 1 h)
MFA biométrique + YubiKey vs. ergonomie	Doubles authentifications à chaque entrée et chaque session	Maintien des deux facteurs ; cycles de session AD calibrés pour limiter l'inconfort ; revue ergonomique semestrielle
Surveillance vidéo et journalisation vs. RGPD / climat social	Acceptabilité humaine, dialogue social, conformité RGPD	PIA conduite, information transparente des salariés, durées de conservation strictes, accès aux enregistrements limité au RSSI et au DPO
Concentration sur 5 habilités vs. continuité	Risque d'indisponibilité humaine majeur (5 personnes)	Polyvalence documentée, dossier d'habilitation d'un réserviste préparé, exercices de remplacement annuels
Sous-traitance vs. souveraineté	Tentation d'externaliser certaines briques (cloud, MSP)	Interdiction du cloud pour Confidencial ; recours à des prestataires français/européens qualifiés ANSSI pour les briques sensibles

Décision d'engagement de la Direction Générale :

Le Directeur Général reconnaît que les dispositifs définis par la présente PSSI constituent le meilleur équilibre actuel entre la protection requise par la classification « Confidencial », la continuité d'activité contractualisée avec SpainTurbine, la performance opérationnelle de la PME et ses contraintes budgétaires. Les risques résiduels qui demeurent malgré ces dispositifs sont documentés, datés et acceptés par décision formelle du Directeur Général après avis du RSSI.

Annexes

Annexe A – Synthèse des dispositifs techniques (extrait du DAT)

Composant	Quantité	Coût unitaire	Coût total
Switch Cisco Catalyst 9200	1	10 000 €	10 000,00 €
Pare-feu Cisco Secure Firewall 1120	1	5 000 €	5 000,00 €
PC employés HP Elite 800 G9	3	1 663,87 €	4 991,61 €
PC mise à jour HP Elite 800 G9	1	1 663,87 €	1 663,87 €
PC chiffrement / déchiffrement HP Elite 800 G9	1	1 663,87 €	1 663,87 €
Serveurs Dell PowerEdge R470 (principal + redondance)	2	30 000 €	60 000,00 €
Station blanche S3Box Hogo	1	5 000 €	5 000,00 €
Coffre-fort Fichet-Bauche Carena 120 L	1	7 500 €	7 500,00 €
Lecteur de bande HPE StoreEver LTO-8 Ultrium 30750	1	6 000 €	6 000,00 €
Lecteur biométrique HID Signo 25B	2	1 600 €	3 200,00 €
Caméra Axis M4216-V	1	750 €	750,00 €
YubiKey C NFC (FIDO U2F/FIDO2)	5	35 €	175,00 €
Cartouches IBM LTO-8 Ultrium 8	15	100 €	1 500,00 €
Verrous USB et RJ45	—	—	120,00 €
Câbles, écrans, accessoires divers	—	—	1 836,00 €
Coffre-fort 6 compartiments à serrures à code	1	500 €	500,00 €
TOTAL			109 400,35 €

Annexe B – Cycle de vie des incidents : schéma synthétique

Le processus interne de gestion des incidents se lit comme suit, en cohérence avec le § 6.1 :

- Phase 1 – Préparation : Gouverner ▸ Identifier ▸ Protéger.
- Phase 2 – Détection : observation des Événements, distinction « Système / Adversaire ».
- Phase 3 – Traitement Système : System failure ▸ Physical damages ▸ Accidental disclosure (téléchargement / e-mail).
- Phase 3 – Traitement Adversaire : Vulnerability exploitation ▸ Brute force ▸ Elevation of privileges ▸ System configuration alteration ▸ Malware ▸ Phishing ▸ DoS/DDoS.
- Phase 4 – Retour à la phase Préparation après RETEX, notification réglementaire et mise à jour des dispositifs.

Annexe C – Glossaire

Acronyme	Définition
AD	Active Directory
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information
APT	Advanced Persistent Threat
CID-T	Confidentialité, Intégrité, Disponibilité, Traçabilité
COSEC	Comité de Sécurité
DAT	Dossier d'Architecture Technique
DPO	Data Protection Officer (Délégué à la Protection des Données)
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité – Risk Manager
EDR	Endpoint Detection and Response
IAM	Identity and Access Management
IGI 1300	Instruction Générale Interministérielle relative à la protection du secret de la défense nationale
LTO	Linear Tape-Open
MFA	Multi-Factor Authentication
NIS 2	Network and Information Security 2 (Directive UE 2022/2555)
PCA / PRA	Plan de Continuité / Plan de Reprise d'Activité
PKI	Public Key Infrastructure
PSSI	Politique de Sécurité des Systèmes d'Information
RETEX	Retour d'expérience
RGPD	Règlement Général sur la Protection des Données
RPO / RTO / MTPD	Recovery Point Objective / Recovery Time Objective / Maximum Tolerable Period of Disruption
RSSI	Responsable de la Sécurité des Systèmes d'Information
SIEM	Security Information and Event Management
TLS	Transport Layer Security