PLAN DE CONTINUITÉ D'ACTIVITÉ

(PCA)

BIOÉNERGIE TECH

Zone classifiée « Confidencial » – Contrat SpainTurbine

Référence document	PCA-BET-ST-2026-001
Version	1.0
Date	23 mai 2026
Classification	C3 – Sensible
Émetteur	RSSI – BIOÉNERGIE TECH
Validation	Direction Générale – M. Laurent Dubois

Suivi documentaire

Le présent document est un document de niveau 2 dérivé de la PSSI (PSSI-BET-ST-2026-001 §7). Il fait partie du Système de Management de la Sécurité de l'Information (SMSI) de BIOÉNERGIE TECH.

Historique des versions

Version	Date	Auteur	Nature des modifications
0.1	10/05/2026	RSSI	Création – trame initiale
0.5	18/05/2026	RSSI + Admin SI	Intégration BIA et fiches réflexes
0.9	21/05/2026	RSSI + DG	Relecture, validation des objectifs RTO/RPO
1.0	23/05/2026	DG / RSSI	Approbation et entrée en vigueur

Diffusion

Destinataire	Modalité
Direction Générale	Exemplaire signé – coffre DG
RSSI	Exemplaire signé – coffre RSSI
Administrateur SI cloisonné	Version contrôlée intranet sécurisé
Responsable projet SpainTurbine	Version contrôlée intranet sécurisé
DPO	Version contrôlée intranet sécurisé
Membres COSEC et Cellule de Crise	Extrait fiches réflexes – classeur crise
Auditeur externe annuel	Sur demande, sous engagement de confidentialité

Documents de référence

Référence	Intitulé
[REF-1]	PSSI BIOÉNERGIE TECH – PSSI-BET-ST-2026-001 (§7 Continuité d'activité)
[REF-2]	Analyse de risques EBIOS RM – EBIOS-BET-ST-2026-001 (ateliers 1 à 5)
[REF-3]	Dossier d'Architecture Technique – DAT-BET-ST-2026-001
[REF-4]	Cahier des charges contractuel SpainTurbine (mai 2026)
[REF-5]	ISO 22301:2019 – Management de la continuité d'activité

[REF-6]	ISO 27031:2011 – Continuité TIC
[REF-7]	Guide ANSSI – Plan de continuité d'activité, principes et organisation (2013)
[REF-8]	Directive NIS 2 (UE) 2022/2555 transposée
[REF-9]	IGI 1300 – Protection du secret de la défense nationale
[REF-10]	Règlement (UE) 2016/679 – RGPD

1. Préambule et présentation du dispositif

1.1 Objet du document

Le présent Plan de Continuité d'Activité (PCA) formalise l'ensemble des dispositions organisationnelles, humaines, techniques et logistiques mises en place par BIOÉNERGIE TECH pour assurer, en mode dégradé puis en mode nominal, la poursuite des activités critiques nécessaires à l'exécution du contrat SpainTurbine, y compris en cas de sinistre majeur affectant tout ou partie du système d'information cloisonné de la zone classifiée « Confidencial ».

Le PCA répond explicitement à l'exigence portée par la question 10 du cahier des charges de la mission (« Comment assurer la poursuite des activités en cas de perturbation majeure du système d'information ? ») et complète la PSSI [REF-1] qui en pose le cadre normatif et les objectifs.

1.2 Périmètre

Le PCA s'applique :

- à l'ensemble du périmètre projet SpainTurbine de BIOÉNERGIE TECH (zone classifiée « Confidencial ») ;
- aux 5 personnes habilitées intervenant sur ce périmètre (3 employés, 1 administrateur SI, 1 responsable projet), au DG et au RSSI ;
- à l'ensemble des biens essentiels VE1 à VE7 et des 27 actifs supports identifiés dans l'EBIOS RM [REF-2] ;
- aux environnements physiques associés : salle serveur cloisonnée, local LTO sécurisé, ateliers de la zone classifiée, SAS biométrique d'accès, salle open space ;
- aux interfaces avec les parties prenantes contractuelles (SpainTurbine, autorités espagnoles, ANSSI, CNIL, DGA).

Le PCA ne couvre pas le SI corporate de BIOÉNERGIE TECH (couvert par un dispositif distinct), mais documente ses interfaces.

1.3 Objectifs

Le PCA poursuit trois objectifs cumulatifs :

- **Objectif 1 —** garantir la sécurité et la santé des personnels présents sur site en cas de sinistre ;
- **Objectif 2 —** préserver les engagements contractuels envers SpainTurbine (cadence de production, confidentialité, traçabilité), dans la limite des seuils MTPD fixés au §3 ;
- **Objectif 3 —** réduire l'exposition juridique, financière et réputationnelle de BIOÉNERGIE TECH en cas de crise majeure (NIS 2, RGPD, IGI 1300, art. 413-9 CP).

1.4 Articulation avec les autres plans

Plan	Périmètre	Articulation avec le PCA
PSSI	Cadre général de sécurité (politique de niveau 1)	Le PCA met en œuvre le §7 de la PSSI
PRA	Volet technique de reprise du SI cloisonné	Le PCA déclenche le PRA pour le rétablissement technique
Plan de gestion de crise cyber	Gouvernance de la cellule de crise	Volet cellule de crise du PCA

Plan de communication de crise	Communication interne et externe (cf. §7 PCA)	Volet communication du PCA
Plan d'évacuation	Sécurité des personnes (chef d'établissement)	Précédence absolue sur le PCA
Plan de protection des données (RGPD)	Notification CNIL en 72 h	Activé par PCA si donnée personnelle

1.5 Cadre normatif et réglementaire

- Directive NIS 2 (entité essentielle – énergie / industrie de défense)
- IGI 1300 – protection du secret de la défense nationale
- Règlement (UE) 2016/679 – RGPD
- Code pénal article 413-9 (compromission du secret de la défense)
- ISO 22301:2019 – Management de la continuité d'activité
- ISO 27031:2011 – Continuité TIC
- Guide ANSSI 2013 – Plan de continuité d'activité, principes et organisation
- Clauses du contrat SpainTurbine (notification 24 h, RTO ≤ 4 h, MTPD ≤ 72 h)

2. Gouvernance et organisation de la continuité

2.1 Acteurs permanents (hors crise)

Rôle	Titulaire	Responsabilités PCA
Directeur Général (DG)	Laurent DUBOIS	Sponsor du PCA, valide la stratégie de continuité, arbitre le budget, valide la déclaration de crise majeure
RSSI	[Titulaire]	Pilote opérationnel du PCA, met à jour le document, anime les exercices, déclare la crise cyber
DPO	[Titulaire]	Notification CNIL (72 h), arbitrage incidents données personnelles
Administrateur SI cloisonné	[Titulaire]	Met en œuvre les procédures techniques du PRA, mainteneur des sauvegardes LTO-8
Responsable projet SpainTurbine	[Titulaire]	Interface client, point unique de contact avec SpainTurbine et l'ANSC
Responsable des Ressources Humaines	[Titulaire]	Gestion de la polyvalence des habilités, plan de remplacement, soutien psychologique post-crise
COSEC (Comité Sécurité)	DG, RSSI, DPO, Admin, Resp. projet, RH	Revue trimestrielle du PCA, suivi des actions, validation des RETEX

2.2 Structure de crise

BIOÉNERGIE TECH retient un modèle de crise à 3 niveaux articulés autour du RSSI (déclencheur) et du DG (autorité finale).

2.2.1 Cellule de Crise Décisionnelle (CCD)

Rôle	Titulaire	Suppléant
Directeur de crise	DG – Laurent DUBOIS	Directeur Industriel
Conseiller cyber / SI	RSSI	DPO
Conseiller juridique	Cabinet conseil externe (astreinte 24/7)	—
Conseiller communication	Responsable communication	RSSI
Représentant métier	Responsable projet SpainTurbine	Resp. production

Mission : décide de l'activation du PCA, arbitre les options de continuité, autorise les communications externes (clients, autorités, presse), pilote le retour à la normale.

2.2.2 Cellule de Crise Opérationnelle (CCO)

Rôle	Titulaire	Suppléant
Chef cellule	RSSI	Administrateur SI
Pilote technique SI	Administrateur SI cloisonné	Sous-traitant prestataire qualifié
Pilote logistique / sécurité physique	Responsable sécurité (HSE)	Resp. moyens généraux
Référent métier production	Resp. projet SpainTurbine	Chef d'atelier turbines
Référent RH	RRH	Assistant RH

Mission : exécute les fiches réflexes, met en œuvre le PRA, collecte les preuves, tient la main courante de crise.

2.2.3 Cellule de Soutien (CSO)

Constituée à la demande, elle apporte une expertise ponctuelle (juridique externe, expert forensique, assureur cyber, prestataire qualifié PRIS ANSSI, médecin du travail).

2.3 Critères et autorité de déclenchement

Le PCA est déclenché par le RSSI (ou son suppléant), sur la base d'au moins un des critères suivants :

- indisponibilité prévisionnelle d'un service critique > 1 h (cf. matrice §3.4) ;
- compromission ou suspicion de compromission d'un bien essentiel coté 4/4 ;
- déclenchement automatique d'une alerte « critique » par la pile ELK ;
- sinistre physique majeur affectant le bâtiment hébergeant la zone classifiée ;
- indisponibilité simultanée de 2 personnes habilitées ou plus ;
- réception d'une demande de rançon ou d'une menace explicite (incluant tentative de coercition sur un personnel) ;
- demande expresse de la DG, de SpainTurbine ou d'une autorité (ANSSI, ANSC, DGA).

L'escalade vers la Cellule de Crise Décisionnelle est immédiate : DG informé en moins de 30 minutes, CCD réunie (présentielle ou téléphonique) en moins de 1 h.

2.4 Logistique de crise

Ressource	Localisation	Bascule de secours
Salle de crise principale (PC Décisionnel)	Bâtiment principal – Salle direction (3e étage)	Bâtiment nouveau – Salle réunion sécurisée
Salle de crise technique (PC Opérationnel)	Salle réunion adjacente salle serveur	Hôtel partenaire dans un rayon de 5 km (convention)
Annuaire de crise	Coffre RSSI + coffre DG (papier scellé), version numérique chiffrée	accès YubiKey CCD
Moyens de communication hors SI	5 téléphones GSM de crise prépayés (cellule)	Talkies-walkies PMR sur site
Alimentation autonome	Onduleurs 30 min + groupe électrogène mutualisé	Convention de fourniture diesel sous 4 h

Connexion Internet de secours	Routeur 4G/5G LTE dédié, hors SI cloisonné	Liaison fibre opérateur secondaire

3. Bilan d'Impact d'Activité (BIA)

3.1 Méthodologie

Le BIA est construit à partir des 7 valeurs métier (VE1 à VE7) et des 8 événements redoutés (ER1 à ER8) issus de l'EBIOS RM [REF-2]. Chaque activité critique est caractérisée par :

- MTPD (Maximum Tolerable Period of Disruption) – durée maximale tolérable d'interruption au-delà de laquelle l'activité ne peut être restaurée sans dommage majeur ;
- RTO (Recovery Time Objective) – durée maximale visée pour restaurer une activité après interruption ;
- RPO (Recovery Point Objective) – fraîcheur maximale acceptable des données restaurées ;
- MBCO (Minimum Business Continuity Objective) – niveau minimal d'activité requis en mode dégradé.

Ces valeurs sont alignées sur la PSSI §7.1 (RTO ≤ 4 h, RPO ≤ 24 h, MTPD ≤ 72 h) et précisées par activité ci-après.

3.2 Activités critiques (par valeur métier)

ID	Valeur métier / activité	D.I.C.	Criticité
VE1	Production technique CAO/CAM des micro-turbines	3/4/4	Critique
VE2	Gestion contractuelle SpainTurbine (livrables, jalons)	2/4/4	Critique
VE3	Secrets cryptographiques (PKI, AD, LTO, YubiKey)	4/4/4	Critique
VE4	Journalisation et supervision (ELK)	3/4/3	Élevée
VE5	Sauvegardes LTO-8 et processus de restauration	4/4/4	Critique
VE6	Administration et configurations du SI cloisonné	3/4/3	Élevée
VE7	Contrôle d'accès physique et logique de la zone	3/4/3	Élevée

3.3 Impacts en l'absence de PCA

Catégorie d'impact	Évaluation	Commentaire
Contractuel (SpainTurbine)	Critique	Pénalités cadence (≥ 50 k€/mois) ; risque de rupture du contrat 1,2 M€/an au-delà de 72 h

Juridique (IGI 1300, art. 413-9 CP)	Critique	Compromission secret défense ; poursuites pénales personnelles et au titre de l'entreprise
Réglementaire (NIS 2)	Élevé	Sanction administrative jusqu'à 10 M€ ou 2 % CA mondial
Données personnelles (RGPD)	Modéré à Élevé	Habilitations/photos identité ; sanction CNIL jusqu'à 4 % CA mondial
Réputationnel	Élevé	Perte de qualification DGA / ANSC, attractivité commerciale dégradée
Financier	Critique	Cumul pénalités + remédiation + perte CA : > 1 M€ potentiel à 3 mois
Humain et social	Modéré	Stress équipe (49 ETP), risque PSE si rupture contrat

3.4 Matrice RTO / RPO / MTPD par service

Service / actif	RTO	RPO	MTPD	Mode dégradé acceptable
AD (Active Directory)	1 h	24 h	4 h	Comptes locaux d'urgence (admin de secours)
Serveur de fichiers SMBv3 (CAO/CAM)	4 h	24 h	72 h	Bureau d'études papier + plans figés
PKI interne	4 h	24 h	72 h	Suspension délivrance certificats ; usage révocations
ELK (logs et SIEM)	8 h	24 h	72 h	Journalisation locale syslog + analyse manuelle
VM Sauvegarde	1 h	24 h	4 h	Démarrage du serveur de redondance Dell R470
VM Admin (rebond)	2 h	24 h	8 h	Console locale clavier/écran KVM
VM Vidéo (caméra Axis)	4 h	0 (en continu)	24 h	Rondes physiques renforcées (toutes les 30 min)
Contrôle d'accès biométrique HID	1 h	0	4 h	Liste d'accès papier + clé physique scellée
Production atelier turbines	4 h	24 h	72 h	Production papier sur plans figés, suspension

				des opérations sensibles
Chaîne de chiffrement (S3Box, USB)	8 h	—	72 h	Suspension des transferts MAJ

Note : ces valeurs sont volontairement plus exigeantes pour les services dont la perte entraîne un blocage complet (AD, contrôle d'accès, sauvegardes) afin d'éviter une cascade d'effets sur l'ensemble de la chaîne.

4. Stratégies de continuité par scénario

Les stratégies suivantes répondent aux 4 scénarios stratégiques EBIOS [REF-2], complétés par les sinistres physiques, les défaillances techniques et l'indisponibilité RH identifiés au cahier des charges.

4.1 Scénario SS1 – APT étatique via flux de mise à jour (SO1)

Gravité : G4 ; Pertinence : P3 ; Niveau : 12 (Très élevé).

Stratégie : isolement immédiat, basculement vers une chaîne de mise à jour de secours, restauration sur image saine pré-incident.

- Isoler physiquement le PC MAJ et la station blanche S3Box dès la suspicion (rupture du flux Microsoft Update).
- Activer une chaîne de MAJ de secours : médias de mise à jour téléchargés par un PC corporate isolé, vérification SHA-256 hors bande contre un mirroir tiers (ANSSI CERT-FR).
- Bascule des postes employés sur images golden snapshot du serveur de redondance (état T-7 jours) : MBCO = production en mode défensif sans nouvelle MAJ pendant la durée de l'investigation.
- Suspension immédiate des transferts vers le réseau interne ; gel des sauvegardes (LTO en quarantaine, marquage rouge).
- Cellule de soutien : prestataire PRIS ANSSI mobilisé pour forensique sous 4 h ; assureur cyber notifié sous 24 h.
- Communication : notification ANSSI sous 24 h (incident NIS 2), SpainTurbine sous 24 h, suspension contractuelle temporaire négociée.

4.2 Scénario SS2 – Insider coercé / vol de cartouche LTO (SO2)

Gravité : G4 ; Pertinence : P3 ; Niveau : 12 (Très élevé).

Stratégie : confinement RH, restauration sur jeu de sauvegardes vérifiées hors site, reconstitution des secrets cryptographiques.

- Confinement RH : suspension immédiate des accès logiques et physiques du personnel suspecté ; convocation RH + DG ; cellule de soutien psychologique mobilisée.
- Vérification d'intégrité immédiate des LTO restants : contrôle des scellés numérotés, recalcul des hashs SHA-256 stockés hors bande, contrôle vidéo des accès au coffre.
- Restauration depuis le jeu hors site (4 cartouches dans une zone sécurisée dans le premier site..) après vérification croisée à quatre yeux DG + RSSI.
- Reconstitution complète des secrets : renouvellement PKI (révocation et émission), rotation krbtgt deux fois (24 h d'intervalle), réémission YubiKey, changement clés de chiffrement LTO.
- Communication : notification ANSSI + ANSC + DGA sous 24 h, dépôt de plainte (art. 413-9 CP), notification SpainTurbine selon clauses contractuelles défense.
- Activation du programme insider threat : revue de tous les accès sensibles, rotation administrateur, séparation des rôles administration / sauvegardes.

4.3 Scénario SS3 – Ransomware via supply chain station blanche

Gravité : G4 ; Pertinence : P2 ; Niveau : 8 (Élevé).

Stratégie : isolement, restauration depuis LTO immuables, repavage des postes, refus catégorique du paiement.

- Isolement physique du périmètre infecté (déconnexion switch Cisco Catalyst 9200) sous 30 minutes.

- Préservation des preuves : image disque des postes affectés, conservation des logs ELK (export sécurisé).
- Repavage complet des postes employés depuis images de référence (golden images stockées sur LTO hors ligne).
- Restauration des données depuis LTO-8 chiffrées (jeu hors site J-7 dans une zone sécurisée dans le premier site si jeu hebdomadaire compromis), test d'intégrité avant remise en production.
- Refus catégorique du paiement de rançon (politique d'entreprise, conformément aux recommandations ANSSI).
- Communication : notification ANSSI sous 24 h, CNIL sous 72 h (si données personnelles touchées), SpainTurbine sous 24 h.

4.4 Scénario SS4 – Espionnage économique soft (concurrent, OSINT)

Gravité : G3 ; Pertinence : P2 ; Niveau : 6 (Modéré).

Stratégie : pas d'impact de continuité immédiat – pilotage par renseignement, sensibilisation, contre-mesures juridiques.

- Renforcement de la veille (CTI) et de la sensibilisation OSINT du personnel.
- Contrôle des publications externes (LinkedIn, conférences) du personnel habilité.
- Cellule juridique mobilisée pour intenter une action en cas de captation de secret d'affaires.

4.5 Sinistres physiques majeurs (incendie, CHEMICALIA, inondation, vol)

Stratégie : évacuation prioritaire, bascule sur site de secours interne (bâtiment principal), reprise depuis sauvegardes délocalisées dans une zone sécurisée dans le premier site sous 72 h.

- Activation du Plan d'évacuation – priorité absolue sur la sauvegarde des personnes.
- Mise à l'abri immédiate des cartouches LTO en cours d'utilisation (coffre Fichet-Bauche ignifuge Carena 120 L) ; coffre conçu pour résister à 1 h de feu standard.
- Périmètre de sécurité étendu en cas d'incident CHEMICALIA (40 m) : confinement, suivi des alertes ICPE, coupure ventilation salle serveur.
- Reprise sur site de secours interne (bâtiment principal historique) : zone tampon préfabriquée prête à recevoir les matériels de remplacement.
- Marché-cadre PRA avec intégrateur qualifié SecNumCloud (livraison serveur Dell PowerEdge équivalent sous 48 h).
- Restauration depuis les 4 cartouches LTO délocalisées dans une zone sécurisée dans le premier site (RPO ≤ 1 semaine sur le pire cas).
- Communication : maire (PPRT/ICPE), préfecture, assurance dommages, ANSSI si impact SI.

4.6 Défaillances techniques (serveur, électricité, climatisation)

Stratégie : redondance à chaud, autonomie énergétique, supervision préventive.

- Serveur principal Dell R470 : bascule automatique à chaud sur serveur de redondance R470 sous 15 minutes.
- Coupure électrique : onduleurs 30 min ; bascule groupe électrogène mutualisé sous 5 min ; convention de réapprovisionnement diesel sous 4 h.
- Perte de climatisation salle serveur : seuil critique à 30 °C, alerte ELK + sonde indépendante ; procédure d'arrêt propre en moins de 15 minutes pour préserver les serveurs ; intervention maintenance sous 4 h (contrat).

- Vieillissement du parc : programme de remplacement serveur principal planifié (cf. EBIOS Vague 1) – à exécuter dès Q3 2026 pour réduire ce risque résiduel.

4.7 Indisponibilité RH (habilités, administrateur SI)

Stratégie : polyvalence documentée, réserviste habilité, séparation des rôles.

- 5 personnes habilitées « Confidencial » sur le périmètre : matrice de polyvalence documentée, mise à jour trimestrielle par le RRH.
- Réserviste habilité : 1 ingénieur en cours d'habilitation maintenue à jour, mobilisable sous 5 jours ouvrés.
- SPOF administrateur SI (cf. EBIOS V2.6) : séparation des rôles administration/sauvegardes mise en place avant fin Q3 2026 ; rotation trimestrielle ; quatre yeux obligatoire sur ouverture coffre LTO.
- Compte de secours administrateur (break glass) scellé au coffre DG, journalisé, contrôle quatre yeux DG+RSSI à chaque usage.
- Astreinte 24/7 RSSI + Admin SI : roulement entre titulaire et suppléant.
- Soutien psychologique post-crise (cellule médecine du travail + prestataire externe sous convention).

5. Fiches réflexes

Les fiches réflexes sont consultables sur format papier dans le classeur de crise (salle de crise principale et coffre RSSI) et en version numérique chiffrée. Elles formalisent les 5 premières minutes, les 30 premières minutes et les 2 premières heures de chaque acteur clé.

5.1 Fiche réflexe – RSSI (déclencheur)

Horizon	Action
T+0 à T+5 min	Confirmer l'incident (cf. matrice §3.4) ; déclarer l'activation du PCA ; alerter le DG par téléphone (numéro de crise)
T+5 à T+15 min	Convoquer la Cellule de Crise Opérationnelle (CCO) ; ouvrir la main courante numérotée ; activer la salle de crise technique
T+15 à T+30 min	Notifier l'Administrateur SI pour exécution du PRA (cf. PRA §4) ; appeler le prestataire PRIS ANSSI (astreinte)
T+30 min à T+1 h	Briefer la CCD ; valider avec le DG la communication SpainTurbine ; activer le plan de communication (§7)
T+1 h à T+2 h	Coordonner les actions techniques et métier ; valider les premières remédiations ; tenir à jour la main courante toutes les 15 min
Au-delà	Reporter toutes les heures à la CCD ; préparer la notification ANSSI (24 h) ; planifier le RETEX

5.2 Fiche réflexe – Directeur Général

Horizon	Action
T+0 à T+15 min	Accuser réception de l'alerte RSSI ; rejoindre la salle de crise décisionnelle ; valider la déclaration de crise majeure
T+15 à T+30 min	Convoquer la CCD au complet ; valider le périmètre d'information interne (équipes opérationnelles uniquement)
T+30 min à T+2 h	Décision sur la communication SpainTurbine (24 h) et autorités ; arbitrage budgétaire (PRA intégrateur, prestataire forensique)
T+2 h à T+4 h	Validation des décisions opérationnelles ; relations institutionnelles (préfecture si sinistre majeur)
Au-delà	Suivi des indicateurs ; communication écrite formelle aux clients critiques ; activation police d'assurance cyber

5.3 Fiche réflexe – Administrateur SI cloisonné

Horizon	Action
T+0 à T+5 min	Confirmer le périmètre technique impacté ; isoler les composants suspects (déconnexion physique switch si nécessaire)
T+5 à T+30 min	Lancer la procédure PRA correspondante (cf. PRA §4) ; collecter les premières preuves (logs ELK, images mémoire)
T+30 min à T+1 h	Préparer la restauration LTO (jeu vérifié hors site) ; rendre compte au RSSI toutes les 15 min
T+1 h à T+4 h	Exécuter la restauration (cf. runbooks PRA) ; test d'intégrité avant remise en service
Au-delà	Documenter les actions effectuées dans la main courante ; transmettre les éléments forensique au prestataire PRIS

5.4 Fiche réflexe – Responsable projet SpainTurbine

Horizon	Action
T+0 à T+30 min	Rejoindre la CCO ; identifier les livrables contractuels affectés (jalons en cours, expéditions prévues)
T+30 min à T+1 h	Préparer le message technique pour SpainTurbine ; rester silencieux jusqu'à validation DG/CCD
T+1 h à T+24 h	Appel formel au point de contact SpainTurbine (responsable contrat) à l'issue de la décision CCD ; remonter l'ANSC
Au-delà	Coordonner le rattrapage planning ; négociation des avenants ou pénalités ; production de reportings hebdomadaires

5.5 Fiche réflexe – DPO

Horizon	Action
T+0 à T+1 h	Évaluer l'impact sur les données personnelles (habilitations, photos, badges, vidéo SAS)
T+1 h à T+24 h	Préparer la notification CNIL (si données personnelles touchées) ; documenter le registre des violations
T+24 h à T+72 h	Notification CNIL (CNIL.fr formulaire) ; communication aux personnes concernées si risque élevé
Au-delà	Suivi des mesures correctives ; mise à jour de l'AIPD ; intégration au registre

5.6 Fiche réflexe – Responsable RH

Horizon	Action
T+0 à T+1 h	Vérifier la présence et l'intégrité physique de tout le personnel habilité ; activer le canal RH de crise
T+1 h à T+4 h	Mobiliser la polyvalence si indisponibilité ; activer le réserviste si nécessaire (>5 j)
T+4 h à T+24 h	Mobiliser le soutien psychologique (médecine du travail, prestataire externe) en cas d'incident traumatisant
Au-delà	Suivi RH post-crise ; ajustement de la matrice de polyvalence ; intégration au RETEX RH

6. Modes de fonctionnement dégradés (MBCO)

6.1 Atelier turbines (production)

- Plans CAO/CAM figés à T-24 h (dernier export papier de référence) – mise à disposition sur supports papier signés et numérotés.
- Suspension des opérations sensibles nécessitant un certificat numérique (chiffrement) jusqu'à restauration PKI.
- Production en mode séquentiel manuel avec pointage papier ; intégration ultérieure dans le SI au retour à la normale.
- Activité maximale en mode dégradé : ~ 60 % de la cadence nominale (estimation), tenable au plus 72 h.

6.2 Contrôle d'accès (zone Confidencial)

- Bascule sur liste d'accès papier validée par le RSSI ; vérification visuelle + badge nominatif tamponné.
- Renforcement des rondes physiques (toutes les 30 min) ; tenue d'un registre d'entrée/sortie horodaté.
- Compte rendu quotidien à la DG.

6.3 Communication SI

- Téléphones GSM de crise (5 unités prépayées) pour les membres CCD/CCO – numéros répertoriés dans l'annuaire de crise.
- Talkies-walkies PMR sur site (canal dédié crise) pour la coordination physique inter-bâtiments.
- Liaison 4G/5G LTE de secours pour les communications externes (jamais connectée au SI cloisonné).

6.4 Sauvegardes en mode dégradé

- Sauvegarde manuelle quotidienne sur LTO hors ligne pendant la phase de reprise (incrémentale forcée chaque soir).
- Vérification d'intégrité (hash SHA-256) systématique avant rotation.
- Conservation temporaire de 2 jeux supplémentaires en coffre dans une zone sécurisée dans le premier site, jusqu'à validation de la sortie de crise.

7. Plan de communication de crise

7.1 Principes

- Toute communication externe est validée par le DG (CCD) ; aucune sortie unilatérale.
- Un porte-parole unique est désigné (DG ou Responsable communication) pour la presse et les autorités.
- Cohérence des messages : un message « fait » et un message « action » au minimum ; pas de spéculation publique sur les causes.
- Préservation du secret défense : aucune mention publique des éléments classifiés.

7.2 Matrice des parties prenantes et délais

Destinataire	Canal	Délai	Responsable	Contenu type
Direction Générale	Téléphone de crise	Immédiat (< 30 min)	RSSI	Nature, périmètre, premières mesures
Cellule de Crise	Téléphone + salle de crise	< 1 h	RSSI	Convocation, briefing factuel
Personnel habilité (5 ETP)	Présentiel + RH	< 2 h	RRH + DG	Consignes, sécurité, soutien
SpainTurbine	Téléphone + lettre recommandée	< 24 h	Resp. projet + DG	Nature de l'incident, impact contractuel, mesures
ANSSI (NIS 2)	Formulaire CERT-FR	< 24 h (alerte précoce)	RSSI	Notification incident significatif
ANSC (autorité espagnole)	Voie diplomatique / contractuelle	< 24 h	Resp. projet + DG	Selon clauses contrat défense
DGA (le cas échéant)	Officier de sécurité DGA	< 24 h si secret défense	RSSI + DG	Notification IGI 1300 si compromission
CNIL (RGPD)	Formulaire en ligne CNIL	< 72 h si données perso	DPO	Notification de violation
Autorités judiciaires	Plainte / dépôt avocat	< 7 j si vol/cyber	DG + cabinet	Plainte article 413-9, 323-1 et s. CP
Préfecture / Mairie	Téléphone + courrier	Sinistre physique	DG	Si déclenchement ICPE / PPRT
Assureur cyber	Téléphone + portail	< 24 h	DG	Activation police
Personnel non habilité	Note interne RH	< 24 h	RRH	Rassurer, consignes minimales
Presse (si exposition)	Communiqué validé CCD	Si saisine média	Resp. communication + DG	Faits validés uniquement

7.3 Trame de notification SpainTurbine (24 h)

Modèle structuré à compléter et faire valider par la CCD :

- Identité de l'émetteur, référence du contrat, date et heure de détection.

- Nature de l'incident (qualification technique non sensible : « indisponibilité partielle », « compromission suspectée », sans divulgation TTP).
- Périmètre affecté (sans mention des éléments classifiés).
- Impact contractuel évalué (jalons impactés, cadence prévisible).
- Mesures de remédiation déjà engagées, sans détail technique sensible.
- Calendrier prévisionnel de retour à la normale.
- Engagement de transmettre des points d'avancement (toutes les 12 h pendant la phase aiguë).

7.4 Trame de notification ANSSI (24 h)

Soumission par formulaire CERT-FR (selon NIS 2 – alerte précoce) :

- Identité de l'entité, code APE, secteur (industrie de défense / énergie).
- Catégorisation de l'incident (compromission, indisponibilité, atteinte intégrité, atteinte confidentialité).
- Impact estimé (utilisateurs touchés, services touchés, durée prévisible).
- TTP suspectées (le cas échéant), IoC déjà identifiés.
- Demande d'assistance CERT-FR le cas échéant.
- Rapport intermédiaire sous 72 h, rapport final sous 1 mois conformément NIS 2.

8. Maintien en condition opérationnelle (MCO) du PCA

8.1 Revue documentaire

- Revue trimestrielle en COSEC (mise à jour des contacts, des actifs, des contrats fournisseurs).
- Revue annuelle complète par le RSSI ; validation par la DG.
- Revue exceptionnelle après tout changement structurant (nouvel actif critique, nouveau personnel habilité, nouveau client, changement contractuel).

8.2 Programme d'exercices

Type d'exercice	Périodicité	Pilote	Périmètre	Livrable
Tabletop cyber	Semestrielle	RSSI	CCD + CCO – scénario tournant (SS1, SS2, SS3)	Compte rendu RETEX + plan d'action
Exercice de continuité complet	Annuelle	RSSI + DG	Simulation grandeur nature (8 h)	RETEX, mise à jour du PCA
Test de restauration partielle LTO	Hebdomadaire	Admin SI	1 cartouche par semaine, fichiers échantillons	PV de test signé
Test de restauration complète LTO	Mensuelle	Admin SI + RSSI	Restauration intégrale sur serveur de test	PV contresigné DG + RSSI
Exercice évacuation site	Annuelle	HSE	Évacuation bâtiments	Compte rendu réglementaire
Exercice insider / coercition	Annuelle	RSSI + RH	Détection comportements anormaux, quatre yeux coffres	RETEX dédié programme insider
Test communication SpainTurbine	Annuelle	Resp. projet	Test de la chaîne d'appel et de notification	PV de test

8.3 Indicateurs de pilotage du PCA

Indicateur	Objectif	Périodicité	Responsable
Taux de réussite des tests de restauration LTO	≥ 95 %	Mensuelle	Admin SI
Délai moyen d'activation du PCA (exercice)	≤ 1 h	Annuelle	RSSI
Délai moyen de bascule serveur principal/redondance	≤ 15 min	Semestrielle	Admin SI
Nombre de personnes habilitées disponibles (matrice polyvalence)	≥ 5 / 5	Trimestrielle	RRH

Délai moyen de notification SpainTurbine en exercice	≤ 24 h	Annuelle	Resp. projet
Taux de couverture des fiches réflexes à jour	100 %	Trimestrielle	RSSI
Écart entre RTO théorique et RTO observé en exercice	≤ +10 %	Annuelle	RSSI
Taux de participation aux exercices	≥ 90 %	Annuelle	RRH

8.4 Plan d'amélioration continue

Aligné sur les vagues du plan d'action EBIOS (V1 à V3, ~180 k€ sur 12 mois) :

- Vague 1 (≤ 3 mois) : déploiement test restauration hebdomadaire (MT-09), scellés numérotés LTO (MP-03), formalisation matrice polyvalence (MO-02).
- Vague 2 (≤ 6 mois) : délocalisation des clés LTO hors site (huissier/banque – MP-06), séparation des rôles admin/sauvegarde, déploiement quatre yeux ouverture coffres.
- Vague 3 (≤ 12 mois) : renouvellement serveur principal, automatisation des hashs SHA-256 hors bande, intégration site de secours géographiquement distant (à étudier).

9. Retour à la normale et clôture de crise

9.1 Critères de clôture

- Tous les services critiques (cf. matrice §3.4) sont restaurés à un niveau supérieur à 95 % de la nominale pendant au moins 24 h.
- Aucune alerte critique nouvelle dans la pile ELK depuis 24 h.
- Validation explicite de la CCD (DG + RSSI au minimum) après revue contradictoire.
- Pour les scénarios SS1/SS2/SS3 : avis favorable du prestataire forensique sur l'absence de persistance.

9.2 Procédure de clôture

- Bascule officielle en mode nominal (note CCD signée DG).
- Reprise progressive des activités sensibles (PKI, chiffrement, transferts) avec supervision renforcée pendant 7 jours.
- Levée de la cellule de crise ; conservation des éléments de preuve dans le coffre RSSI (durée légale).
- Réunion de RETEX (cf. §9.3) sous 15 jours.

9.3 Retour d'expérience (RETEX)

Le RETEX est obligatoire après toute activation du PCA (exercice ou réelle). Il est piloté par le RSSI et comporte au minimum :

- Description factuelle de l'incident (chronologie horodatée à partir de la main courante).
- Décisions prises (qui, quand, justification).
- Indicateurs observés vs objectifs (RTO/RPO/MTPD réels).
- Difficultés rencontrées et causes racines.
- Plan d'action correctif (porteurs et échéances).
- Présentation au COSEC pour validation et au DG pour information.

10. Annexes

Annexe A – Annuaire de crise (squelette)

La version nominative est conservée sous forme papier scellée au coffre DG et au coffre RSSI, et sous forme chiffrée sur l'intranet sécurisé. Format de la version diffusée ci-dessous :

Rôle	Titulaire	Suppléant	Téléphone fixe	GSM crise	Email sécurisé
DG – Directeur de crise	L. Dubois	[Dir. Industriel]	[●]	[●]	[●]
RSSI – Chef CCO	[●]	[●]	[●]	[●]	[●]
DPO	[●]	[●]	[●]	[●]	[●]
Admin SI cloisonné	[●]	[●]	[●]	[●]	[●]
Resp. projet SpainTurbine	[●]	[●]	[●]	[●]	[●]
RRH	[●]	[●]	[●]	[●]	[●]
Responsable HSE	[●]	[●]	[●]	[●]	[●]
Resp. communication	[●]	[●]	[●]	[●]	[●]
Astreinte prestataire PRIS	[Société]	—	[●]	[●]	[●]
Assureur cyber – cellule incident	[Société]	—	[●]	[●]	[●]
Cabinet juridique	[Société]	—	[●]	[●]	[●]
Point contact SpainTurbine	[●]	[●]	[●]	[●]	[●]
CERT-FR (ANSSI)	—	—	01 71 75 84 50	—	cert-fr.cossi@ssi.gouv.fr
CNIL	—	—	01 53 73 22 22	—	—

Annexe B – Modèle de main courante de crise

N°	Horodatage	Auteur	Source	Événement / décision	Suivi
001	JJ/MM AAAA HH:MM	RSSI	ELK	Alerte critique sur AS06 – exfiltration suspectée	→ activation PCA
002	JJ/MM AAAA HH:MM	RSSI	Téléphone	Appel DG, activation PCA validée	→ CCD convoquée

003	JJ/MM AAAA HH:MM	Admin SI	Console	Isolation switch Cisco	—
[…]	—	—	—	—	—

Annexe C – Glossaire

Acronyme	Signification
BIA	Business Impact Analysis – Bilan d'Impact d'Activité
CCD / CCO / CSO	Cellule de Crise Décisionnelle / Opérationnelle / de Soutien
COSEC	Comité Sécurité (instance trimestrielle de pilotage)
DAT	Dossier d'Architecture Technique
EBIOS RM	Expression des Besoins et Identification des Objectifs de Sécurité (méthode ANSSI)
IoC	Indicator of Compromise – marqueur de compromission
LTO-8	Linear Tape-Open génération 8 – format de bande magnétique
MBCO	Minimum Business Continuity Objective
MCO	Maintien en Condition Opérationnelle
MTPD	Maximum Tolerable Period of Disruption
PCA / PRA	Plan de Continuité / de Reprise d'Activité
PKI	Public Key Infrastructure – infrastructure à clé publique
PRIS	Prestataire de Réponse aux Incidents de Sécurité (qualifié ANSSI)
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SS / SO	Scénario Stratégique / Opérationnel (EBIOS RM)
SPOF	Single Point of Failure – point unique de défaillance
TTP	Tactics, Techniques and Procedures
VE	Valeur Essentielle (ou Valeur métier dans EBIOS RM)

Annexe D – Approbation

Rôle	Nom	Date	Signature

Émetteur – RSSI	[Titulaire RSSI]	23/05/2026
Validation – DPO	[Titulaire DPO]	23/05/2026
Approbation – Directeur Général	Laurent DUBOIS	23/05/2026