PLAN DE REPRISE D'ACTIVITÉ

(PRA)

BIOÉNERGIE TECH

Volet technique de reprise du SI cloisonné « Confidencial » – Contrat SpainTurbine

Référence document	PRA-BET-ST-2026-001
Version	1.0
Date	23 mai 2026
Classification	C3 – Sensible
Émetteur	RSSI + Administrateur SI cloisonné
Validation	Direction Générale – M. Laurent Dubois

Suivi documentaire

Document de niveau 2 du SMSI de BIOÉNERGIE TECH, dérivé de la PSSI §7 et complémentaire du PCA (PCA-BET-ST-2026-001).

Historique des versions

Version	Date	Auteur	Nature des modifications
0.1	12/05/2026	Admin SI	Trame initiale, runbooks bruts
0.5	18/05/2026	Admin SI + RSSI	Intégration de la procédure LTO et des images de référence
0.9	21/05/2026	RSSI	Relecture, alignement RTO/RPO avec PCA, test des runbooks
1.0	23/05/2026	DG / RSSI	Approbation, entrée en vigueur

Documents de référence

Référence	Intitulé
[REF-1]	PSSI BIOÉNERGIE TECH (§7 Continuité d'activité)
[REF-2]	EBIOS RM BIOÉNERGIE TECH (ateliers 1 à 5)
[REF-3]	Dossier d'Architecture Technique – DAT
[REF-4]	PCA BIOÉNERGIE TECH – PCA-BET-ST-2026-001
[REF-5]	ISO 22301:2019 / ISO 27031:2011
[REF-6]	Guide ANSSI PRA TIC (2013, mise à jour 2024)
[REF-7]	Documentation constructeurs (Dell PowerEdge R470, HPE StoreEver LTO-8, Cisco Catalyst 9200, Cisco Secure FW 1120, S3Box Hogo)

Sommaire

(Table des matières dynamique – clic droit > Mettre à jour les champs.)

1. Préambule et périmètre

1.1 Objet du document

Le présent Plan de Reprise d'Activité (PRA) décrit l'ensemble des dispositions techniques permettant de rétablir le système d'information cloisonné « Confidencial » de BIOÉNERGIE TECH après un incident majeur, dans les délais (RTO) et avec la fraîcheur de données (RPO) attendus par le PCA et le contrat SpainTurbine.

Il fournit, pour chaque scénario significatif issu de l'analyse EBIOS RM et du cahier des charges, les procédures opérationnelles (« runbooks ») à exécuter par l'Administrateur SI cloisonné sous le pilotage du RSSI.

1.2 Périmètre technique

Le PRA s'applique aux composants techniques de la zone classifiée :

- 3 sous-réseaux isolés : Réseau interne, Réseau de chiffrement, Réseau de mise à jour ;
- 2 serveurs Dell PowerEdge R470 (principal + redondance) hébergeant 7 VM (PKI, AD, ELK, Partage SMBv3, Vidéo, Admin rebond, Sauvegarde) ;
- Switch Cisco Catalyst 9200 et pare-feu Cisco Secure Firewall 1120 ;
- 5 postes : 3 PC HP Elite 800 G9 employés, 1 PC MAJ, 1 PC chiffrement ;
- Lecteur HPE StoreEver LTO-8 Ultrium 30750 et 15 cartouches IBM LTO-8 ;
- Station blanche S3Box Hogo, 2 lecteurs biométriques HID Signo 25B, caméra Axis M4216-V, 5 YubiKey C NFC FIDO2 ;
- Coffre-fort Fichet-Bauche Carena 120 L et coffre à 6 compartiments (clés et YubiKey de recouvrement).

1.3 Hypothèses de planification

- Les bandes LTO-8 du jeu hors site (dans une zone sécurisée dans le premier site) sont supposées disponibles et intègres ; un mécanisme de fallback est prévu si compromises.
- Le serveur de redondance Dell R470 est maintenu en bascule à chaud (cluster actif/passif).
- Au moins un administrateur SI ou son suppléant est disponible dans un délai de 1 h.
- Le prestataire PRIS ANSSI est mobilisable sous 4 h via le contrat d'astreinte.
- Les sauvegardes sont chiffrées matériellement (HPE Ultrium) et un hash SHA-256 hors bande est disponible pour vérification d'intégrité (à déployer Vague 1 EBIOS).

1.4 Stratégie générale de reprise

Le PRA repose sur quatre niveaux de reprise, choisis selon le scénario et la criticité :

Niveau	Mode de reprise	Cas d'usage	RTO cible
N1	Bascule à chaud (cluster)	Défaillance serveur principal, VM unique	≤ 15 min
N2	Restauration depuis LTO en ligne (jeu hebdomadaire courant)	Corruption logique, suppression accidentelle	≤ 4 h
N3	Restauration depuis LTO hors site (dans une zone sécurisée dans le premier site..)	Compromission jeu courant, sinistre local	≤ 24 h
N4	Reconstruction complète (images golden + intégrateur)	Sinistre majeur (incendie, ransomware total)	≤ 72 h

2. Objectifs RTO / RPO / MTPD techniques

Les objectifs ci-après sont contractualisés via la PSSI §7.1 et le PCA §3.4. Ils s'imposent à l'administrateur SI et constituent le critère de validation de tout test de restauration.

Composant / Service	Criticité	Niveau	RTO	RPO	MTPD
AD (Active Directory)	Critique	N1 / N2	1 h	24 h	4 h
Serveur de fichiers SMBv3 (CAO/CAM)	Critique	N2 / N3	4 h	24 h	72 h
PKI interne	Critique	N2 / N3	4 h	24 h	72 h
ELK (logs)	Élevée	N2 / N3	8 h	24 h	72 h
VM Sauvegarde	Critique	N1	1 h	24 h	4 h
VM Admin (rebond)	Élevée	N1 / N2	2 h	24 h	8 h
VM Vidéo (caméra)	Élevée	N1	4 h	0	24 h
Contrôle d'accès biométrique HID	Critique	N1	1 h	0	4 h
Switch / Firewall	Critique	N1 (matériel de spare)	2 h	—	8 h
Lecteur LTO-8 (HPE)	Critique	N3 / N4	24 h	—	72 h
Station blanche S3Box	Élevée	N2 / N4	8 h	—	72 h

3. Architecture de reprise

3.1 Schéma logique de bascule

Le SI cloisonné repose sur un cluster actif/passif (serveur principal Dell R470 ↔ serveur redondance R470) complété par un coffre Fichet-Bauche LTO sur site et un jeu hors site dans une zone sécurisée dans le premier site.. Les images « golden » des VM critiques (AD, PKI, ELK, SMB, Admin, Vidéo, Sauvegarde) sont conservées sur LTO immuables (write-once WORM) avec rotation grand-père / père / fils sur 4 semaines.

3.2 Inventaire des sauvegardes

Type	Fréquence	Support	Localisation	Rétention
Complète (full)	Hebdomadaire (vendredi 20:00)	LTO-8 chiffrée matériel	Coffre Fichet-Bauche Carena 120 L sur site	4 semaines actives + archives mensuelles
Incrémentale	Quotidienne (00:30)	LTO-8 chiffrée matériel	Coffre Fichet-Bauche sur site	7 jours
Délocalisée hors site	Hebdomadaire (lundi)	4 cartouches LTO-8 chiffrées	Coffre siège DG (transport sécurisé)	Rolling 4 semaines
Image golden VM	À chaque changement majeur (Q)	LTO-8 WORM + clone sur SAN local	Coffre Fichet-Bauche + clone serveur redondance	Versionning 4 dernières releases
Configuration équipements	Hebdomadaire + à chaque changement	Fichier chiffré GPG sur LTO + clone sur Admin VM	Coffre + Admin VM	12 mois
Logs ELK	Continue (Logstash)	Stockage Elasticsearch + export LTO mensuel	Sur disques + LTO	12 mois en ligne + 24 mois LTO

3.3 Identification des jeux de sauvegarde

- Étiquetage normalisé : « BET-ST-AAAA-MM-JJ-{FULL|INCR|GOLD}-NNN » + numéro de scellé.
- Empreinte SHA-256 publiée à chaque rotation et conservée hors bande (registre papier + coffre DG).
- Vérification croisée à quatre yeux (Admin SI + RSSI ou DG) lors de chaque dépôt/retrait coffre.
- Registre des accès au coffre tenu en parallèle (papier + numérique).

3.4 Prérequis de reprise (à maintenir disponibles)

- 1 serveur de redondance Dell R470 alimenté et synchronisé en permanence.
- 1 lecteur LTO-8 fonctionnel (test mensuel de tête de lecture).
- 2 jeux complets de cartouches LTO-8 vierges (spare) pour rotation d'urgence.
- Stock de matériel critique : 1 disque SSD/NVMe spare, 1 alimentation serveur spare, 1 switch Catalyst 9200 spare, 1 firewall 1120 spare (cf. EBIOS Vague 2).
- Images golden des VM (Windows AD, Linux ELK, etc.) signées et hashées.
- Documentation à jour des configurations (firewall, switch, AD, PKI) chiffrée et stockée en LTO + coffre RSSI.
- Contrat d'astreinte intégrateur qualifié pour livraison serveur sous 48 h.

4. Procédures opérationnelles (Runbooks)

Chaque runbook suit la trame standard : Déclencheur → Préparation → Exécution → Vérification → Communication. Les runbooks sont à exécuter par l'Administrateur SI sous supervision RSSI, à quatre yeux pour toute action irréversible.

4.1 Runbook R-01 – Bascule serveur principal vers serveur de redondance (N1)

Déclencheur : défaillance matérielle ou logicielle du serveur principal détectée par ELK ou perte de service AD/SMB.

RTO cible : 15 minutes. RPO : ≤ 5 min (réplication continue cluster).

Étape 1 — Confirmer la perte de service sur la console ELK et avec l'outil de monitoring matériel iDRAC.

Étape 2 — Vérifier l'état de santé du serveur de redondance (LED frontal, ping, réplication à jour).

Étape 3 — Activer la bascule cluster : commande administrative depuis console de redondance.

Étape 4 — Vérifier l'enregistrement DNS, la réponse AD (test login) et la disponibilité SMB.

Étape 5 — Notifier le RSSI ; mettre à jour la main courante.

Étape 6 — Lancer le diagnostic du serveur principal défaillant ; planifier la remise en service (RTO secondaire 24 h).

Étape 7 — Programmer le retour en mode nominal (cluster actif/passif) après remplacement et tests.

4.2 Runbook R-02 – Restauration depuis LTO en ligne (N2)

Déclencheur : corruption logique d'un partage de fichiers, suppression accidentelle confirmée.

RTO cible : 4 h. RPO : ≤ 24 h (incrémentale).

Étape 1 — Geler les écritures sur la VM impactée (mode lecture seule) pour préserver l'état.

Étape 2 — Récupérer la bande de référence : Admin SI + RSSI accèdent au coffre Fichet-Bauche (quatre yeux).

Étape 3 — Vérifier le scellé numéroté et le hash SHA-256 hors bande.

Étape 4 — Monter la bande sur le lecteur HPE LTO-8 ; lancer la restauration de la VM ou des fichiers ciblés.

Étape 5 — Test d'intégrité post-restauration : comparaison des hashs des fichiers restaurés vs. registre d'intégrité.

Étape 6 — Remettre la VM en mode lecture/écriture après validation RSSI.

Étape 7 — Documenter dans la main courante : bande utilisée, durée, taille restaurée, anomalies.

4.3 Runbook R-03 – Restauration depuis LTO hors site (N3)

Déclencheur : suspicion de compromission du jeu courant (ransomware, sabotage interne) ou destruction du coffre sur site.

RTO cible : 24 h. RPO : ≤ 1 semaine (jeu hebdomadaire délocalisé).

Étape 1 — Décision formelle de la CCD (DG + RSSI) ; consignation au PV de crise.

Étape 2 — Récupération des 4 cartouches au siège DG, sous escorte sécurisée (transport en valise scellée et journalisée).

Étape 3 — Vérification quatre yeux des scellés et hashs SHA-256 hors bande.

Étape 4 — Mise en quarantaine du jeu courant suspect (étiquetage rouge, mise en coffre séparé).

Étape 5 — Restauration complète sur serveur de redondance préalablement repavé (image golden vérifiée).

Étape 6 — Reconstitution des secrets : rotation krbtgt deux fois (intervalle 24 h), réémission certificats PKI, renouvellement clés LTO.

Étape 7 — Tests fonctionnels avant ouverture au métier : login AD, lecture/écriture SMB, traçabilité ELK, accès biométrique HID.

Étape 8 — Reprise progressive sous supervision renforcée (logs ELK contrôlés en temps réel pendant 7 j).

4.4 Runbook R-04 – Reconstruction complète (N4)

Déclencheur : sinistre majeur (incendie, ransomware total, destruction physique du site).

RTO cible : 72 h. RPO : ≤ 1 semaine.

Étape 1 — Activation de la convention intégrateur qualifié (livraison serveur Dell R470 équivalent et lecteur HPE LTO-8 sous 48 h).

Étape 2 — Mise en place de la zone tampon de secours dans le bâtiment principal (préfabriqué + alimentation + climatisation).

Étape 3 — Restauration de l'environnement à partir des images golden hors site + LTO délocalisées.

Étape 4 — Reconfiguration des équipements réseau (switch Cisco, firewall Cisco) depuis configurations sauvegardées chiffrées.

Étape 5 — Reconstitution complète des secrets cryptographiques (PKI, AD krbtgt, clés LTO, YubiKey).

Étape 6 — Sanity check end-to-end : utilisateurs habilités testent les fonctions clés en environnement contrôlé.

Étape 7 — Bascule officielle vers le nouvel environnement (signature DG + RSSI).

Étape 8 — Programmation du retour au site nominal après remise en état (3 à 6 mois).

4.5 Runbook R-05 – Incident APT via chaîne de MAJ (SS1)

Déclencheur : alerte ELK sur comportement anormal post-MAJ (DCSync, .lnk suspect, exfiltration DoH), ou signalement CERT-FR.

RTO cible : 8 h (isolement) + 24 h (restauration) + 72 h (durcissement).

Étape 1 — Isoler immédiatement le PC MAJ et la station blanche S3Box (déconnexion physique).

Étape 2 — Conserver les preuves : image disque (FTK Imager ou dd), capture mémoire (volatility), logs ELK chiffrés.

Étape 3 — Suspendre les flux de mise à jour ; activer la chaîne de MAJ de secours (PC corporate isolé + vérification SHA-256 hors bande contre CERT-FR mirror).

Étape 4 — Lancer une recherche d'IoC sur l'ensemble du SI cloisonné (recherche YARA fournie par PRIS, vérification des hashs binaires, analyse trafic DNS sortant).

Étape 5 — Restauration des postes employés depuis images golden T-7 jours (Runbook R-02 ou R-03 selon état des sauvegardes).

Étape 6 — Rotation krbtgt deux fois (intervalle 24 h), réémission YubiKey, audit complet des comptes AD (Bloodhound).

Étape 7 — Patch / contournement de la CVE exploitée (ex. CVE-2024-38112) ; mise à jour de la baseline durcie.

Étape 8 — Notification ANSSI (24 h) ; remontée d'IoC au CERT-FR.

Étape 9 — RETEX dans les 15 jours ; mise à jour des règles de détection ELK (signatures comportementales, DoH, .lnk).

4.6 Runbook R-06 – Vol/substitution de cartouche LTO (SS2)

Déclencheur : scellé brisé constaté, anomalie test de restauration, signalement d'un personnel.

RTO cible : 24 h (restauration depuis hors site) + 72 h (durcissement).

Étape 1 — Geler immédiatement l'accès au coffre Fichet-Bauche (changement combinaison + nouvelle clé).

Étape 2 — Vérifier l'intégrité de toutes les cartouches restantes : contrôle scellés + recalcul SHA-256.

Étape 3 — Récupérer les images vidéo Axis du SAS; les exporter chiffrées vers un support hors ligne.

Étape 4 — Confinement RH : suspension immédiate des accès logiques (révocation YubiKey, désactivation compte AD) et physiques (carte biométrique) du personnel suspecté.

Étape 5 — Activer le Runbook R-03 (restauration depuis hors site).

Étape 6 — Lancer la procédure de reconstitution des secrets (cf. PCA §4.2) : PKI, AD krbtgt, clés LTO, YubiKey.

Étape 7 — Saisine immédiate des autorités : ANSSI (NIS 2), ANSC, DGA, dépôt de plainte (art. 413-9 CP).

Étape 8 — Renforcement insider : mise en place du quatre yeux obligatoire pour ouverture coffre, scellés numérotés, déplacement des clés LTO hors site (dans une zone sécurisée dans le premier site..).

4.7 Runbook R-07 – Ransomware (SS3)

Déclencheur : chiffrement constaté de fichiers, note de rançon, anomalie ELK (entropie élevée, suppression de shadow copies, processus suspect).

RTO cible : 30 min (isolement) + 4 h (restauration partielle) + 24 h (restauration complète).

Étape 1 — Isolement physique du périmètre : déconnexion du switch Cisco Catalyst 9200 (ports correspondants).

Étape 2 — Préservation des preuves : capture mémoire et image disque des postes infectés (cf. Runbook R-05 étape 2).

Étape 3 — Identification du variant (souche, version) via outil ID Ransomware ou prestataire PRIS.

Étape 4 — Décision formelle : pas de paiement (politique d'entreprise). Notification ANSSI et assureur cyber.

Étape 5 — Repavage complet des postes employés depuis images golden (Runbook R-02 si jeu courant sain, R-03 si compromis).

Étape 6 — Restauration des données depuis LTO immuable (jeu hors site si jeu courant chiffré).

Étape 7 — Test d'intégrité avant remise en production (hash + scan AV-EDR à jour + relance contrôlée).

Étape 8 — Renforcement préventif : durcissement station blanche (mise à jour signatures, ajout sandbox dynamique), désactivation USB sur tous les postes non MAJ, rotation des secrets exposés.

Étape 9 — Surveillance renforcée pendant 30 j (ELK avec règles spécifiques à la souche).

4.8 Runbook R-08 – Indisponibilité de l'administrateur SI (RH)

Déclencheur : indisponibilité programmée ou subite de l'administrateur titulaire.

RTO cible : 2 h (bascule sur suppléant).

Étape 1 — Activer le suppléant administrateur (cf. matrice de polyvalence RH) – contact via annuaire de crise.

Étape 2 — Vérifier la validité de ses droits AD, YubiKey, accès biométrique et coffre.

Étape 3 — Si suppléant indisponible : utiliser le compte break glass (scellé coffre DG, quatre yeux DG+RSSI obligatoire).

Étape 4 — Mobiliser le réserviste habilité si indisponibilité > 5 jours ouvrés.

Étape 5 — Activer la cellule de soutien (médecine du travail si nécessaire).

Étape 6 — RETEX RH sous 15 jours pour ajustement matrice polyvalence.

4.9 Runbook R-09 – Sinistre physique salle serveur (incendie, dégât eaux)

Déclencheur : alerte incendie, dégât des eaux, accident industriel CHEMICALIA (40 m).

RTO cible : 72 h pour reprise complète.

Étape 1 — Priorité absolue : évacuation des personnes (Plan d'évacuation HSE).

Étape 2 — Confinement automatique salle serveur (extinction gaz inerte, coupure ventilation).

Étape 3 — Mise en sécurité des bandes LTO en cours d'utilisation (coffre Fichet-Bauche ignifuge déjà sur site).

Étape 4 — Constat dommages dès accès rétabli ; périmètre de sécurité maintenu jusqu'à expertise.

Étape 5 — Activer Runbook R-04 (reconstruction complète) en parallèle de la déclaration sinistre.

Étape 6 — Mise en service de la zone tampon dans le bâtiment principal.

Étape 7 — Reprise progressive selon ordre de priorité (cf. §2 : AD → SMB → ELK).

Étape 8 — Communication assureur dommages, préfecture, ICPE le cas échéant.

4.10 Runbook R-10 – Coupure électrique générale

Déclencheur : coupure secteur détectée par les onduleurs (alarme).

RTO cible : N/A (continuité onduleurs + groupe).

Étape 1 — T+0 : onduleurs prennent le relais automatiquement (30 min d'autonomie).

Étape 2 — T+5 min : démarrage automatique du groupe électrogène mutualisé.

Étape 3 — T+15 min : vérification stabilité tension, confirmation visuelle du groupe et niveau de carburant.

Étape 4 — Si coupure > 30 min : information CCO ; bascule arrêt propre des services non critiques pour économiser les onduleurs.

Étape 5 — T+4 h : approvisionnement diesel selon convention (autonomie maintenue jusqu'à retour secteur).

Étape 6 — Retour secteur : bascule contrôlée vers le réseau ; tests onduleurs (charge batterie).

Étape 7 — Si arrêt forcé subi : appliquer Runbook R-01 ou R-02 selon état des serveurs.

5. Tests et validations

5.1 Plan de test annuel

Test	Périodicité	Pilote	Objectif	Critère de réussite
Test de lecture LTO (échantillon)	Hebdomadaire	Admin SI	Lire 1 cartouche aléatoire	Hash conforme + lecture sans erreur
Restauration partielle (fichiers)	Hebdomadaire	Admin SI	Restaurer 100 fichiers échantillons	RTO < 30 min, intégrité 100 %
Restauration complète VM	Mensuelle	Admin SI + RSSI	Restaurer la VM SMB sur serveur de test	RTO < 4 h, fonctionnement OK
Bascule cluster R-01	Trimestrielle	Admin SI	Failover/failback contrôlé	RTO < 15 min, aucune perte
Restauration LTO hors site (R-03)	Annuelle	Admin SI + RSSI + DG	Restaurer un jeu complet depuis une zone sécurisée dans le premier site	RTO < 24 h, intégrité 100 %
Reconstruction complète (R-04)	Annuelle (tabletop + drill partiel)	Admin SI + intégrateur	Simuler livraison serveur + restauration	Temps < 72 h sur scénario théorique
Exercice ransomware (R-07)	Annuelle	RSSI + Admin SI	Drill avec souche de test isolée	Détection < 15 min, isolement < 30 min
Exercice break glass admin (R-08)	Annuelle	DG + RSSI	Ouverture du compte de secours en condition	Procédure quatre yeux exécutée, traçabilité 100 %
Test groupe électrogène (R-10)	Mensuelle	HSE / Maintenance	Démarrage à blanc 15 min	Démarrage < 5 min, tension stable

5.2 Documentation des tests

- Pour chaque test, un PV est rédigé (modèle Annexe B).
- PV mensuel et annuel contresigné DG + RSSI.
- Conservation 5 ans (audit ANSSI / certification éventuelle).
- Indicateurs consolidés au COSEC trimestriel.

5.3 Critères de réussite globaux

- Taux de succès des tests > 95 % sur l'année glissante.
- Écart entre RTO observé et RTO objectif < 10 %.
- Aucune perte de données au-delà du RPO objectif.
- 100 % des PV signés dans les 7 jours suivant le test.

6. Maintien en condition opérationnelle (MCO) du PRA

6.1 Mise à jour

- Mise à jour systématique à chaque changement d'architecture (ajout/retrait de composant, mise à jour majeure).
- Revue trimestrielle des runbooks par le RSSI et l'Admin SI.
- Validation annuelle complète en COSEC.

6.2 Indicateurs PRA

Indicateur	Cible	Périodicité
Taux de réussite tests restauration	≥ 95 %	Mensuelle
Délai moyen restauration LTO (RTO)	≤ 4 h	Mensuelle
Délai moyen bascule cluster	≤ 15 min	Trimestrielle
Disponibilité du SI cloisonné (MTBF)	≥ 99,5 %	Trimestrielle
Couverture des runbooks (à jour)	100 %	Trimestrielle
Stock de spares matériels	100 %	Mensuelle
Délai d'intervention prestataire PRIS	≤ 4 h	À chaque sollicitation

6.3 Plan d'amélioration

Aligné sur les vagues du plan d'action EBIOS [REF-2] :

- Vague 1 (≤ 3 mois) : test restauration hebdomadaire (MT-09), scellés numérotés LTO (MP-03), hashs SHA-256 hors bande automatisés (MT-08), runbook break glass formalisé.
- Vague 2 (≤ 6 mois) : délocalisation des clés LTO chez huissier (MP-06), spares matériels supplémentaires (switch, FW), séparation rôles admin/sauvegardes (MO-02).
- Vague 3 (≤ 12 mois) : renouvellement serveur principal vieillissant, sandboxing dynamique sur station blanche, étude site de secours géographiquement distant.

7. Annexes

Annexe A – Cartographie des sauvegardes (vue synthétique)

VM / Composant	Stratégie	Localisation primaire	Localisation hors site
AD	Full hebdo + incr. quotidiennes + image golden	LTO sur site (Fichet-Bauche)	LTO dans une zone sécurisée dans le premier site..
PKI	Full hebdo + image golden + sauvegarde clé root (HSM)	Coffre RSSI + LTO sur site	LTO dans une zone sécurisée dans le premier site + duplicata clé root coffre depuis une zone sécurisée dans le premier site..
ELK	Snapshot Elasticsearch + export LTO mensuel	Disque local + LTO sur site	LTO depuis une zone sécurisée dans le premier site
Partage SMBv3 (CAO/CAM)	Full hebdo + incr. quotidiennes	LTO sur site	LTO depuis une zone sécurisée dans le premier site
VM Vidéo (Axis)	Snapshot + sauvegarde des enregistrements 30 j	Disque local + LTO	LTO depuis une zone sécurisée dans le premier site
VM Admin (rebond)	Image golden + sauvegarde config	LTO + clone serveur redondance	LTO depuis une zone sécurisée dans le premier site
VM Sauvegarde	Bootstrap minimal sur LTO + script de reconstruction	LTO sur site	LTO depuis une zone sécurisée dans le premier site
Configuration Switch / Firewall	Export hebdomadaire chiffré GPG	Admin VM + LTO	LTO depuis une zone sécurisée dans le premier site

Annexe B – Modèle de PV de test de restauration

Champ	Valeur
Date / heure du test	JJ/MM/AAAA HH:MM
Type de test	Partiel / Complet / R-XX
Composants couverts	[liste]
Bande(s) utilisée(s)	[étiquettes + scellés]
Hash vérifié	OUI / NON / NA
RTO observé	[hh:mm]
RTO cible	[hh:mm]
RPO observé	[hh:mm]
Anomalies rencontrées	[texte]
Actions correctives	[texte]
Signature Admin SI	

Signature RSSI	
Signature DG (si test complet)	

Annexe C – Matrice de correspondance scénarios / runbooks

Scénario EBIOS / sinistre	Runbook(s) à exécuter
SS1 – APT via flux MAJ (SO1)	R-05 puis R-02 ou R-03
SS2 – Insider coercé / vol LTO (SO2)	R-06 puis R-03
SS3 – Ransomware via supply chain	R-07 puis R-02 ou R-03
SS4 – Espionnage économique soft	Pas de PRA technique – traitement par PSSI / juridique
Défaillance serveur principal	R-01
Sinistre majeur (incendie, CHEMICALIA)	R-09 + R-04
Coupure électrique	R-10
Indisponibilité admin SI	R-08
Corruption / suppression accidentelle	R-02

Annexe D – Inventaire matériel critique de spare

Catégorie	Modèle / quantité	Localisation	Délai de mobilisation
Serveur de redondance	Dell PowerEdge R470 × 1 (à chaud)	Salle serveur	Immédiat (failover)
Disques NVMe spares	× 2	Coffre matériel	< 30 min
Alimentation serveur	× 1	Coffre matériel	< 30 min
Switch	Cisco Catalyst 9200 × 1	Stock IT	< 1 h
Firewall	Cisco Secure Firewall 1120 × 1	Stock IT	< 1 h
Lecteur LTO-8	HPE StoreEver LTO-8 Ultrium 30750 × 1 (spare)	Stock IT	< 1 h
Cartouches LTO-8 vierges	× 10	Coffre Fichet-Bauche	< 5 min
YubiKey de recouvrement	× 2 (DG + RSSI)	Coffre 6 compartiments	< 5 min
Onduleurs	× 2 (redondance N+1)	Salle serveur	Automatique
Groupe électrogène	Mutualisé site (Diesel)	Local énergie	T+5 min auto

Annexe E – Procédure d'accès aux coffres (quatre yeux)

- Toute ouverture du coffre Fichet-Bauche ou du coffre à 6 compartiments est soumise à la règle des quatre yeux (deux personnes parmi DG / RSSI / Admin SI).
- Inscription préalable sur le registre d'accès papier (date, heure, motif, personnes).

- Levée des scellés numérotés sur les cartouches LTO : photographie horodatée des scellés avant et après.
- Tout accès est journalisé dans la pile ELK (intégration HID + caméra Axis).
- Revue trimestrielle du registre par le RSSI ; remontée en COSEC.

Annexe F – Glossaire technique

Terme	Définition
Cluster actif/passif	Configuration où un serveur est actif et un autre en veille synchronisée (failover automatique)
DCSync	Technique d'extraction de hashs AD via le protocole de réplication (MITRE T1003.006)
Golden image	Image système de référence validée et signée, conservée hors ligne
HSM	Hardware Security Module – module matériel de protection de clés cryptographiques
krbtgt	Compte AD utilisé pour signer les tickets Kerberos – rotation = invalidation des Golden Tickets
LTO-8 WORM	Cartouche Linear Tape-Open génération 8, Write-Once Read-Many (non-réinscriptible)
RPO	Recovery Point Objective – fraîcheur maximale acceptable des données restaurées
RTO	Recovery Time Objective – délai maximal de restauration d'un service
Runbook	Procédure opérationnelle détaillée, pas-à-pas, pour traiter un type d'incident
SHA-256	Algorithme d'empreinte cryptographique (256 bits) pour vérification d'intégrité
WORM	Write Once Read Many – média non-réinscriptible (protection ransomware)
YubiKey FIDO2	Authentificateur matériel multi-facteurs (clé USB / NFC)

Annexe G – Approbation

Rôle	Nom	Date	Signature
Émetteur – Administrateur SI	[Titulaire]	23/05/2026	
Co-émetteur – RSSI	[Titulaire]	23/05/2026	

Approbation – Directeur Général	Laurent DUBOIS	23/05/2026