SIRA-TECH

INFOGÉRANCE · CYBERSÉCURITÉ · CLOUD PRIVÉ

Les 12 contrôles de résilience d'un système d'information

Adaptés aux réalités de l'Afrique de l'Ouest :
électricité, chaleur, connectivité, pièces de rechange

Diagnostic gratuit de 30 minutes

Guide de terrain — septembre 2026
Côte d'Ivoire · Sénégal · Burkina Faso · Mali · Bénin · Togo
+225 07 08 36 30 94 · contact@sira-tech.com · sira-tech.com

Contrôles 1 à 6 — le socle

1 Électricité : coupures absorbées

Onduleurs et inverseurs testés, autonomie connue, arrêt propre des serveurs et des applications sensibles. Une coupure ne doit jamais se transformer en corruption de données.

2 Chaleur, humidité, poussière

Local technique tempéré, filtres entretenus, température surveillée avec alerte avant la panne. La chaleur tue les disques plus vite que l'âge.

3 Lien principal et lien de secours

Fibre, 4G ou radio : bascule automatique et testée, pour que la coupure de connectivité ne devienne pas un arrêt d'activité.

4 Sauvegardes hors du site

Trois copies des données, sur deux supports différents, dont une hors site ou hors ligne (règle 3-2-1), y compris pour les sites secondaires.

5 Restauration réellement testée

Une restauration complète effectuée et documentée, sur un environnement isolé — pas une sauvegarde dont on suppose qu'elle fonctionne.

6 Double facteur sur les accès

Messagerie, VPN, consoles d'administration et applications métier protégées par MFA. Le mot de passe volé reste la première porte d'entrée.

Contrôles 7 à 12 — la maîtrise dans le temps

7 Comptes à privilèges maîtrisés

Administrateurs nominatifs, aucun compte partagé, revue régulière des droits, retrait immédiat des accès des personnes qui quittent l'entreprise.

8 Postes et messagerie protégés

Antivirus ou EDR géré, filtrage des pièces jointes et de l'hameçonnage, sensibilisation des équipes aux arnaques au faux président et aux faux appels bancaires.

9 Correctifs de sécurité suivis

Systèmes, hyperviseurs, pare-feu et applications : un plan de mise à jour avec fenêtre de sécurité, malgré les contraintes de bande passante.

10 Supervision 24/7 utile

Des alertes hiérarchisées qui remontent à une astreinte humaine, avec seuils définis, historique et rapport mensuel : pas une boîte mail que personne ne consulte.

11 Documentation et pièces de rechange

Schéma d'architecture à jour, procédures, coffre de mots de passe, contacts d'escalade et inventaire des pièces critiques à garder en stock.

12 Plan de reprise (PRA / PCA)

RTO et RPO écrits, procédure connue des équipes, exercice de reprise effectué au moins une fois par an, et sauvegardes restaurables hors du site principal.

Et maintenant ?

Un seul point manquant suffit à transformer un incident en arrêt d'activité. En 30 minutes, nous passons ces 12 contrôles en revue avec vous et vous remettons les 3 risques à traiter en premier, par écrit et sans engagement.

Sira-Tech — Infogérance & Cybersécurité, France & Afrique de l'Ouest
Lieusaint (France) · Abidjan (Côte d'Ivoire)
+225 07 08 36 30 94 · 06 19 27 44 38 · contact@sira-tech.com · https://www.sira-tech.com