Le mirador
SERVICE D'INFOGÉRANCE SÉCURISÉ

CYBERSÉCURITÉ · PLAN POUR PME

CYBERSÉCURITÉ OPTIMALE.

Plan en 9 étapes

Sur la base des 18 contrôles du Center for Internet Security (CIS), Référence a élaboré un plan de cybersécurité assurant une couverture adaptée aux besoins des PME et à coût raisonnable.

RÉFÉRENCE SYSTÈMES Intégration TI · Cybersécurité · Solutions cloud

FONCTION	CONTRÔLES DU CIS	ÉLÉMENT DE CYBERSÉCURITÉ	PRATIQUES ATTENDUES	PRODUITS ET SERVICES OFFERTS PAR RÉFÉRENCE
IDENTIFIER	1 2 3 5	**Gestion des actifs et des comptes**	Maintenir un inventaire des appareils, logiciels et comptes; réviser trimestriellement; désactiver les entrées non autorisées.	RMM Datto Mirador Bastion
IDENTIFIER	3	**Classification des données**	Étiqueter les données comme Publiques, Internes ou Sensibles; assurer une manipulation, un stockage et élimination appropriés.	Microsoft Purview
PROTÉGER	4 6 10 14	**Configuration sécurisée et formation**	Appliquer les références de sécurité CIS, supprimer les mots de passe par défaut, activer les pare-feux et former les employés.	Mirador Bastion
PROTÉGER	6	**Contrôle d'accès et MFA**	Mettre en œuvre le MFA pour l'accès administrateur et à distance; appliquer le principe du moindre privilège.	Watchguard | Fortinet SonicWall | Sophos
PROTÉGER	9 10	**Protection contre les courriels et logiciels malveillants**	Utiliser des filtres anti-pourriel, antivirus et navigateurs sécurisés; appliquer les correctifs chaque semaine.	Hornet Security | Eset
PROTÉGER	3 11	**Protection et sauvegarde des données**	Chiffrer les données au repos et en transit; tester les sauvegardes trimestriellement.	Mirador Bastion | Veeam
DÉTECTER	7 8 13	**Gestion des vulnérabilités et des journaux**	Automatiser les analyses de vulnérabilités mensuelles; examiner les journaux de sécurité chaque semaine.	Mirador Bastion EDR | MDR divers
RÉPONDRE	17	**Réponse aux incidents**	Documenter et tester le plan de réponse aux incidents une fois par an.	Mirador Bastion EDR | MDR divers
RÉCUPÉRER	11	**Récupération des données**	Vérifier la restauration des sauvegardes deux fois par an; définir les objectifs de temps de récupération.	Mirador Bastion | Veeam

RÉFÉRENCE CIS

Contrôles du CIS

1 Inventaire matériel
2 Inventaire logiciel
3 Protection des données
4 Configuration sécurisée
5 Gestion des comptes
6 Contrôle d'accès
7 Gestion des vulnérabilités
8 Journaux d'audit
9 Protection e-mail / web
10 Anti-malware
11 Sauvegardes/récupération
12 Infrastructure réseau*
13 Surveillance réseau
14 Sensibilisation utilisateurs
15 Fournisseurs / tiers*
16 Sécurité applicative*
17 Réponse aux incidents
18 Tests d'intrusion*

**Ces critères ne sont pas utilisés dans notre plan de cybersécurité pour PME, car ils conviennent davantage aux grandes entreprises.*