Liste de contrôle de la sécurité en ligne

Organisation :	
Date :	
Vérificateur :	
Poste :	

Remarque : *La liste de contrôle suivante fournit un formulaire permettant d'identifier les points « élémentaires » de cybersécurité. Cette liste n'est en aucun cas une liste complète de contrôle des expositions aux risques. Une réponse « Non » à l'un des points suivants peut indiquer un besoin de prendre des mesures supplémentaires de sécurité ou de gestion des risques.*

Administratif

LISTE DE CONTRÔLE	OUI	NON	S.O.	DESCRIPTION/RECOMMANDATIONS
1. Il existe des directives écrites concernant :				
• la protection des données ;	○	○	○	
• la protection de la confidentialité des données ;	○	○	○	
• les attentes en matière de confidentialité ;	○	○	○	
• la surveillance des problèmes de confidentialité ;	○	○	○	
• la limitation de l'accès et de l'utilisation des données ;	○	○	○	
• les exigences et la gestion des mots de passe ;	○	○	○	
• « Apportez votre propre appareil » (BYOD) ;	○	○	○	
• La gestion des incidents en matière de sécurité ;	○	○	○	
• La publication dans les médias sociaux et la gestion de ceux-ci.	○	○	○	
2. La fédération ou toute autre entité juridique dispose d'une cyberassurance qui couvre l'organisation.	○	○	○	
3. Il existe une procédure de vérification des contrôles de sécurité de tiers qui ont accès à de quelconques données personnelles.	○	○	○	

Inventaire

LISTE DE CONTRÔLE	OUI	NON	S.O.	DESCRIPTION/RECOMMANDATIONS
1. Liste de tous les matériels et logiciels utilisés.	○	○	○	
2. Tous les logiciels non essentiels ont été supprimés des appareils du ministère.	○	○	○	
3. Quelqu'un est chargé tous les ans de faire le suivi du matériel et des logiciels du ministère.	○	○	○	
4. Inventaire de tous les éléments technologiques susceptibles de stocker ou de traiter des informations, qu'ils soient connectés ou non au réseau.	○	○	○	

Gestion des utilisateurs et des mots de passe

LISTE DE CONTRÔLE	OUI	NON	S.O.	DESCRIPTION/RECOMMANDATIONS
1. Tous les réseaux sans fil sont protégés par un mot de passe.	○	○	○	
2. Les mots de passe par défaut de tous les systèmes ont été modifiés.	○	○	○	
3. Un cryptage WPA2 doit être configuré pour les réseaux sans fil.	○	○	○	
4. Les utilisateurs ont été informés de leur responsabilité concernant la protection de leurs mots de passe et de leurs comptes.	○	○	○	
5. Établissement de comptes, autorisations et mots de passe séparés entre administrateur et opérateurs.	○	○	○	
6. Tous les mots de passe sont différents et répondent à l'exigence minimale de 12 caractères alphanumériques.	○	○	○	
7. L'authentification multifacteur (MFA ou 2FA) a été activée sur tous les comptes, ce qui permet d'offrir cette couche de sécurité supplémentaire.	○	○	○	
8. Les comptes utilisateurs et l'accès au réseau ou aux données ont été configurés en utilisant la règle du moindre privilège, laquelle accorde l'accès au niveau nécessaire pour ne permettre que les actions autorisées.	○	○	○	
9. Les comptes privilégiés ont été révisés et restreints, si nécessaire.	○	○	○	
10. Les personnes disposant d'un accès privilégié ont signé un contrat d'utilisation et ont été soumises à une vérification de leurs antécédents.	○	○	○	
11. Les comptes inutilisés ont été supprimés.	○	○	○	
12. Les informations d'identification et de comptes partagés ont été répertoriées, et il existe un document indiquant qui en a accès (les comptes partagés sont déconseillés).	○	○	○	
13. Lorsque cela est possible, seules les autorisations basées sur les fonctions sont implémentées.	○	○	○	

Connectivité

LISTE DE CONTRÔLE	OUI	NON	S.O.	DESCRIPTION/RECOMMANDATIONS
1. Tous les appareils connectés à l'Internet des objets (IdO) se trouvent sur un segment de réseau distinct (VLAN ou réseau invité) qui n'a pas accès aux ressources internes.	◯	◯	◯	
2. Tous les accès des fournisseurs ont été supprimés lorsqu'ils ne sont pas en usage actif.	◯	◯	◯	
3. Tout accès Internet passe par un pare-feu.	◯	◯	◯	
4. Les utilisateurs invités n'ont accès qu'à un réseau sans fil indépendant, et les appareils invités ne peuvent pas se connecter à d'autres appareils invités sur ce réseau indépendant.	◯	◯	◯	
5. Les utilisateurs invités ne peuvent pas accéder aux périphériques internes.	◯	◯	◯	

Accès physique

LISTA DE VERIFICACIÓN	SÍ	NO	N/A	DESCRIPCIÓN / RECOMENDACIÓN
1. Il existe un document indiquant qui contrôle l'accès à tous les lieux où sont placés tous les équipements, y compris les locaux électriques, mécaniques et des communications.	◯	◯	◯	
2. Il existe un document indiquant la façon dont est obtenu l'accès aux lieux où sont placés les équipements, y compris l'accès en dehors des heures ouvrées.	◯	◯	◯	
3. La sécurité physique des composants du système est confirmée dans le cadre de la procédure d'inventaire.	◯	◯	◯	
4. Les appareils non autorisés, tels que les appareils mobiles personnels, ne peuvent pas accéder aux réseaux internes.	◯	◯	◯	

Sensibilisation

LISTE DE CONTRÔLE	OUI	NON	S.O.	DESCRIPTION/RECOMMANDATIONS
1. Les utilisateurs ont été formés et avertis sur les risques liés à l'installation de nouveaux logiciels liés au travail du ministère (par exemple : des jeux, chats, applications d'achat, etc.).	○	○	○	
2. Tous les membres du personnel qui interagissent avec les ordinateurs du ministère reçoivent au moins une fois par an une formation de sensibilisation à la cybersécurité.	○	○	○	
3. Les utilisateurs ont signé un accord contre une mauvaise utilisation des appareils ou de l'accès à l'Internet du ministère.	○	○	○	

Procédés

LISTE DE CONTRÔLE	OUI	NON	S.O.	DESCRIPTION/RECOMMANDATIONS
1. Pour tous les appareils et systèmes, il existe un plan de réponse documenté contre les cyberincidents.	○	○	○	
2. Les journaux système sont collectés et révisés, et des mesures appropriées sont prises.	○	○	○	
3. Tous les systèmes sont mis à jour automatiquement, avec les derniers correctifs installés lors de leur publication.	○	○	○	
4. Tous les logiciels sont mis à jour automatiquement, avec les derniers correctifs installés lors de leur publication.	○	○	○	
5. Les pare-feu sont activés sur tous les appareils.	○	○	○	
6. Tous les systèmes exécutent un logiciel antivirus mis à jour régulièrement.	○	○	○	
7. Tous les systèmes qui ne peuvent plus être mis à jour ou corrigés sont supprimés du réseau.	○	○	○	

Proceso

LISTE DE CONTRÔLE	OUI	NON	S.O.	DESCRIPTION/RECOMMANDATIONS
8. Les sauvegardes hors connexion sont utilisées et testées au moins une fois par trimestre.	○	○	○	
9. Tous les appareils et lecteurs mobiles sont cryptés.	○	○	○	
10. Toutes les connexions à Internet sont filtrées pour empêcher l'accès aux logiciels malveillants ou au contenu indésirable sur le réseau ou les systèmes du ministère.	○	○	○	
11. Les branchements aux données réseau inutilisés sont débranchés de celui-ci, ils ne peuvent donc pas être utilisés sans autorisation.	○	○	○	
12. Seuls les services cloud autorisés sont utilisés et leur utilisation est documentée.	○	○	○	