



BÂTISSONS NOTRE SOUVERAINETÉ NUMÉRIQUE

- INITIATIVE
- INNOVATION
- INTÉGRITÉ

## DIRECTIVES DE SECURITE POUR LES ADMINISTRATIONS ET OPERATEURS D'INFRASTRUCTURES CRITIQUES



Conseil



Infrastructure



Transformation  
Digitale



Fréquences



Cybersécurité

- 1. Établir une politique de sécurité complète :** Mettez en place des politiques de sécurité claires pour guider les actions en matière de sécurité informatique.
- 2. Effectuer des évaluations régulières des risques :** Identifiez les vulnérabilités potentielles et mettez en place des mesures correctives.
- 3. Surveiller en continu les activités et les menaces :** Utilisez des outils de surveillance pour détecter et répondre rapidement aux menaces.
- 4. Mettre en place des contrôles d'accès stricts :** Limitez l'accès aux informations sensibles et gérez les identités de manière sécurisée.
- 5. Gérer et protéger les identités :** Utilisez des solutions d'authentification forte et surveillez les activités des utilisateurs.
- 6. Sauvegarder et restaurer les données de manière sécurisée :** Établissez des politiques de sauvegarde et cryptez les données sensibles.
- 7. Former et sensibiliser le personnel :** Fournissez une formation régulière sur la sécurité informatique.
- 8. Mettre à jour et patcher les systèmes et les logiciels :** Assurez-vous que tous les systèmes sont régulièrement mis à jour avec les derniers correctifs de sécurité.
- 9. Planifier et tester les plans de réponse aux incidents :** Développez des plans de réponse aux incidents détaillés et testez-les régulièrement.
- 10. Collaborer avec d'autres équipes et partager les informations sur les menaces :** Travaillez en étroite collaboration avec d'autres équipes et partagez les informations sur les menaces pour renforcer la sécurité globale.