NETWORK INFORMATION SECURITY

LES 23 RÈGLES DE LA DIRECTIVE NIS

NOTA : LA DIRECTIVE NIS 2 / DÉCEMBRE 2022 / ELARGIT LE CHAMP DES RESPONSABILITÉS

GOUVERNANCE

- 1 Analyse de risque
  - Objectif : Réaliser une analyse de risques des systèmes d'information essentiels (SIE) dans le cadre de l'homologation sécurité

GOUVERNANCE

- 2 Politique de Sécurité
  - Objectif : Mise en œuvre d'une politique de sécurité des réseaux et systèmes d'information (PSSI)

GOUVERNANCE

- 3 Homologation de sécurité
  - Objectif : Mise en œuvre d'une procédure d'homologation prévue par une politique de sécurité des réseaux et des systèmes d'information

GOUVERNANCE

- 4 Indicateurs
  - Objectif : Evaluation pour chaque Système d'Information Essentiel des indicateurs, de la méthode d'évaluation et des résultats

GOUVERNANCE

- 5 Audits de Sécurité
  - Objectif : Audit de sécurité de chaque Système d'Information Essentiel dans le cadre de l'homologation de sécurité

GOUVERNANCE

- 6 Cartographie
  - Objectif : Cartographie de chaque Système d'Information Essentiel

PROTECTION

- 7 Configuration
  - Objectif : Respect des règles spécifiques de configuration des Systèmes d'Information Essentiels

PROTECTION

- 8 Cloisonnement
  - Objectif : Cloisonnement des Systèmes d'Information Essentiels afin d'éviter les attaques informatiques

PROTECTION

- 9 Accès Distant
  - Objectif : Protection des accès distants des Systèmes d'Information Essentiels

PROTECTION

- 10 Filtrage
  - Objectif : Mise en place des mécanismes de filtrage des flux de données circulant dans les Systèmes d'Information Essentiels

PROTECTION

- 11 Comptes d'Administration
  - Objectif : Création des comptes d'administration spécifiques aux ressources des Systèmes d'Information Essentiels

PROTECTION

- 12 Système d'Information des administrations
  - Objectif : Gestion et configuration des ressources matérielles et logicielles du sysgtème d'information d'administration

PROTECTION

- 13 Identification
  - Objectif : Création des comptes d'identification spécifiques accédants aux ressources des Systèmes d'Information Essentiels

PROTECTION

- 14 Authentification
  - Objectif : Protection des accès aux ressources des Systèmes d'Information Essentiels grâce à un mécanismes d'authentification spécifique

PROTECTION

- 15 Droits d'Accès
  - Objectif : Mise en place des règles de gestion et d'attribution des droits d'accès spécifiques aux ressources des Systèmes d'Information Essentiels

PROTECTION

- 16 Procédure de maintien en condition de sécurité
  - Objectif : Déploiement d'une procédure de maintien en conditions de sécurité des Systèmes d'Information Essentiels

PROTECTION

- 17 Sécurité physique et environnementale
  - Objectif : Mise en œuvre des procédures de sécurité physique et environnementales des Systèmes d'Information Essentiels

DEFENSE

- 18 Détection
  - Objectif : Détection des incidents de sécurité affectant des Systèmes d'Information Essentiels

DEFENSE

- 19 Journalisation
  - Objectif : Journalisation sur chaque Systèmes d'Information Essentiels

DEFENSE

- 20 Corrélation et analyse des journaux
  - Objectif : Analyse de la journalisation et des événements susceptibles d'affecter la sécurité des Systèmes d'Information Essentiels

DEFENSE

- 21 Réponses aux incidents
  - Objectif : Traitement des incidents de sécurité affectant la sécurité des Systèmes d'Information Essentiels

DEFENSE

- 22 Traitement des alertes
  - Objectif : Mise en place d'un service dédié en relation avec l'ANSSI pour le traitement des alertes affectant des Systèmes d'Information Essentiels

RESILIENCE

- 23 Gestion des crises
  - Objectif : Gestion des crises en cas d'incident de sécurité majeur sur les Systèmes d'Information Essentiels