# LES 23 RÈGLES DE LA DIRECTIVE NIS

## GOUVERNANCE

### 1 ANALYSE DE RISQUES

**Objectif** : réalisation d'une analyse de risques des Systèmes d'Information Essentiels (SIE) dans le cadre de l'homologation de sécurité.

### 2 POLITIQUE DE SÉCURITÉ

**Objectif** : mise en œuvre d'une Politique de Sécurité des réseaux et Systèmes d'Information (PSSI).

### 3 HOMOLOGATION DE SÉCURITÉ

**Objectif** : mise en œuvre d'une procédure d'homologation prévue par une Politique de Sécurité des réseaux et Systèmes d'Information.

### 4 INDICATEURS

**Objectif** : évaluation pour chaque Système d'Information Essentiel des indicateurs, de la méthode d'évaluation et des résultats.

### 5 AUDITS DE SÉCURITÉ

**Objectif** : audit de sécurité de chaque Système d'Information Essentiel dans le cadre de l'homologation de sécurité.

### 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.

### 8 CLOISONNEMENT

**Objectif** : cloisonnement des Systèmes d'Information Essentiels afin de limiter les attaques informatiques.

### 9 ACCÈS DISTANT

**Objectif** : protection des accès distants des Systèmes d'Information Essentiels.

### 10 FILTRAGE

**Objectif** : mise en place des mécanismes de filtrage des flux de données circulant dans les Systèmes d'Information Essentiels.

### 11 COMPTES D'ADMINISTRATION

**Objectif** : création des comptes d'administration spécifiques aux ressources des Systèmes d'Information Essentiels.

### 12 SYSTÈMES D'INFORMATION DES ADMINISTRATIONS

**Objectif** : gestion et configuration des ressources matérielles et logicielles spécifiques du SI d'administration.

### 13 IDENTIFICATION

**Objectif** : création de comptes d'identification spécifiques accédant aux ressources des Systèmes d'Information Essentiels.

### 14 AUTHENTIFICATION

**Objectif** : protection des accès aux ressources des Systèmes d'Information Essentiels grâce à un mécanisme d'authentification spécifique.

### 15 DROITS D'ACCÈS

**Objectif** : mise en place de règles de gestion et d'attribution des droits d'accès spécifiques aux ressources des Systèmes d'Information Essentiels.

### 16 PROCÉDURE DE MAINTIEN EN CONDITIONS DE SÉCURITÉ

**Objectif** : déploiement d'une procédure de maintien en conditions de sécurité des Systèmes d'Information Essentiels.

### 17 SÉCURITÉ PHYSIQUE ET ENVIRONNEMENTALE

**Objectif** : mise en œuvre de procédures de sécurité physique et environnementale des Systèmes d'Information Essentiels.

## DÉFENSE

### 18 DÉTECTION

**Objectif** : détection des incidents de sécurité affectant des Systèmes d'Information Essentiels.

### 19 JOURNALISATION

**Objectif** : journalisation sur chaque Système d'Information Essentiel.

### 20 CORRÉLATION ET ANALYSE DE JOURNAUX

**Objectif** : analyse de la journalisation et des évènements susceptibles d'affecter la sécurité des SIE.

### 21 RÉPONSE AUX INCIDENTS

**Objectif** : traitement des incidents de sécurité affectant ses Systèmes d'Information Essentiels (SIE).

### 22 TRAITEMENT DES ALERTES

**Objectif** : mise en place d'un service dédié en relation avec l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) pour le traitement des alertes.

## RÉSILIENCE

### 23 GESTION DE CRISES

**Objectif** : gestion de crises en cas d'incidents de sécurité ayant un incident de sécurité majeur sur les services essentiels de l'opérateur.

## BESOIN D'AIDE ?

Cabinet de conseil, d'audit et de formation indépendant, MANIKA propose des prestations de Sécurité de l'Information (GRC – Cybersécurité – RGPD), de Résilience (Continuité d'activité – Gestion de crises – Sûreté) et de maîtrise des processus SI.

Nos experts peuvent vous aider dans la définition et la mise en place de votre stratégie de gouvernance.

COMMERCIAL@MANIKA-CONSULTING.COM
PARIS : +33 (0)1 47 49 81 93 LYON : +33 (0)6 84 76 42 92
ROUEN : +33 (0)2 78 77 5 80 ABIDJAN : +225 22 43 18 56

MANIKA