#### CYBERDEF101

Orange Cyber Schoo

# Chapitre 4 - Gouvernance de sécurité

Yann-Arzel

27 juillet 2023

### Gouvernance et management de la sécurité

Introduction

- Organisation des entreprises
- Gouvernance : cadre, méthodologie, objectifs
- Comment raisonne un Responsable de la sécurité de l'information (RSSI)?

Yann-Arzel Chapitre 4 - Gouvernance de sécurité 27 juillet 2023

# Construction de la Politique de sécurité du système d'information

Contenu du texte ce que l'on veut comme par exemple

- Définition d'une politique de sécurité
- Intégration de la politique de sécurité dans la gouvernance du SI

Yann-Arzel Chapitre 4 - Gouvernance de sécurité 27 iuillet 2023 3 /

#### Concept de PSG

La politique générale de sécurité

La politique de sécurité générale (PSG) est généralement basée sur l'architecture de l'ISO/EIC 27001, et donne le cadre général de conformité pour les projets, les organisations sous-jacentes (divisions, filiales), les produits ainsi que l'organisation des responsabilités.

Cette PSG est déclinée en différentes politiques de sécurité par secteurs (souvent structurées par les chapitres de l'ISO/EIC 27001)

- IAM
- Filtrage et sécurité périmétrique
- Détection et rémédiation
- continuité d'activité

### Approche par les risques

Contenu de la politique de sécurité

- Identification des biens essentiels à protéger
- Intégration dans la politique de sécurité

### Exemples de chapitres de PSSI

Contenu de la politique de sécurité

- Gestion de l'administration des équipements
  - protocoles d'accès autorisés : SSHv3, HTTPs, interdiction de TELNET
  - protocoles de supervision autorisés : SNMPv3
- Politique de mot de passe
- Gestion des fournisseurs

## Système de management de la sécurité de l'information : SMSI

Introduction à ISO/EIC 27003

- Présentation de la norme ISO/EIC 27001
- Périmètre de certification
- 3 Mesures de sécurité : ISO/EIC 27002

## Very short intro to ISO/EIC 27001

Introduction à ISO/EIC 27003

Quel est le but d'ISO 27k1? Pourquoi l'utiliser?

#### Périmètre de certification

Introduction à ISO/EIC 27003

- Quel est le périmètre de certification?
- SOA : définition, rôle

# ISO/EIC27002

quelles sont les mesures de sécurité?

- Définition mesures de sécurité
- Exemples

#### Audit de conformité

DASHBOARD niveau de sécurité

#### Exemples:

- nb d'incidents critiques
- % remediation vulnérabilité critiques
- %parc administrés suivant les règles de la politique
- nombre de PKI déployées, %PKI dans les équipes sécurité incluses dans le périmètre de certification
- % de personnes sensibilisées

Yann-Arzel

#### Continuité d'activité : ISO22301

Définitions

- Business Impact Analysis (BIA)
- Business Continuity Plan (BCP)
- Plan de Continuité d'Activité (PCA) / Disaster Recovery Plan (DRP)
- Plan de Reprise d'Activité (PRA)