Liste des guides incontournables de l'ANSSI – public averti

Guide d'hygiène informatique
Parmi les mesures techniques que les entités publiques ou privées doivent prendre pour garantir la sécurité de leurs systèmes d'information, on qualifie les plus simples et élémentaires d'entre elles d'hygiène informatique, car elles sont la transposition dans le monde numérique de règles élémentaires de sécurité sanitaire.
https://www.ssi.gouv.fr/entreprise/guide/guide-dhygiene-informatique/
Public : Les RSSI , DSI et administrateurs

Guide d'élaboration d'une charte d'utilisation des moyens informatiques et des outils numériques
Ce guide à destination des petites et moyennes entreprises (PME) et des entreprises de taille intermédiaire (ETI) accompagne l'élaboration d'une charte d'utilisation des moyens informatiques et des outils numériques. 8 points clés pour saisir l'opportunité d'accompagner efficacement la transition numérique des entreprises face à l'augmentation croissante de la menace.
https://www.ssi.gouv.fr/entreprise/guide/guide-delaboration-dune-charte-dutilisation-des-moyens-informatiques-et-des-outils-numeriques/
Public : Les RSSI et DPO

Maîtrise du risque numérique – l'atout confiance
Ce guide propose aux dirigeants et aux risk managers une démarche progressive pour construire étape par étape une politique de gestion du risque numérique au sein de leur organisation.
https://www.ssi.gouv.fr/entreprise/guide/maitrise-du-risque-numerique-latout-confiance/
Public : les décideurs et Risk managers

La méthode EBIOS Risk Manager – Le guide
La méthode EBIOS Risk Manager adopte une approche de management du risque numérique partant du plus haut niveau (grandes missions de l'objet étudié) pour atteindre progressivement les fonctions métier et techniques, par l'étude des scénarios de risque possibles.
https://www.ssi.gouv.fr/entreprise/guide/la-methode-ebios-risk-manager-le-guide/
Public : les Risk managers, RSSI, DSI et chefs de projets

Cartographie du système d'information
Outil indispensable à la maitrise de son système d'information (SI), la cartographie du SI permet de connaitre l'ensemble des éléments qui le constituent pour en obtenir une meilleure lisibilité, et donc un meilleur contrôle. Elle s'intègre dans une démarche globale de gestion des risques.
https://www.ssi.gouv.fr/entreprise/guide/cartographie-du-systeme-dinformation/
Public : Les RSSI , DSI et administrateurs

Recommandations relatives à l'interconnexion d'un système d'information à Internet
Les principes exposés visent à décrire les fonctions de sécurité à mettre en oeuvre dans une passerelle d'interconnexion face aux menaces les plus courantes. Le choix de l'architecture retenue doit être fait au cas par cas en fonction du niveau de sécurité attendu et des contraintes opérationnelles.
https://www.ssi.gouv.fr/entreprise/guide/definition-dune-architecture-de-passerelle-dinterconnexion-securisee/
Public : Les RSSI, DSI et administrateurs

Recommandations pour les architectures des systèmes d'information sensibles ou Diffusion Restreinte
Ce guide donne des recommandations pour la conception de l'architecture des systèmes d'information (SI) qui hébergent des informations sensibles ou Diffusion Restreinte (DR). De manière générale, il apporte des conseils techniques pour la mise en pratique de l'II 901.
https://www.ssi.gouv.fr/administration/guide/recommandations-pour-les-architectures-des-systemes-dinformation-sensibles-ou-diffusion-restreinte/
Public : Les RSSI, DSI et administrateurs