Formation des délégués à la protection des données personnelles (DPO) 2022

Élaboration du plan d'action sécurité et de la politique de protection des données personnelles

Emery Kouassi Assogba, PhD

Novotel, Déc 2022

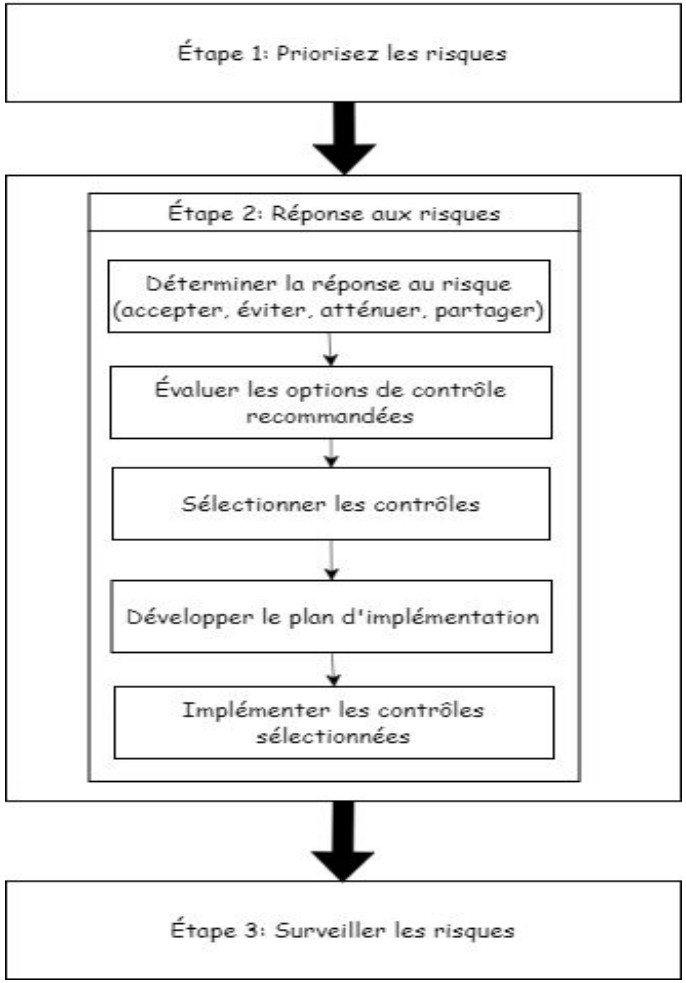
Introduction

L'évaluation des risques d'un SI, d'une organisation identifie les domaines qui ont un besoin d'un traitement. Les PSSI donnent des directives. Les contrôles de sécurité d'un SI, aident à réduire les risques et à mettre en œuvre les directives de la PSSI..

Objectifs

Après avoir suivi cette section, vous devriez être en mesure de :

- Lister les différentes catégories et types de mesures de protection disponibles.
- Décrire le processus de sélection des mesures de protection appropriées pour faire face aux risques.
- Décrire un plan de mise en œuvre pour traiter les risques identifiés.
- Comprendre la nécessité d'un suivi continu de la mise en œuvre de la sécurité.



Contrôle: une action, un dispositif, une procédure ou autre mesure permettant de réduire le risque en éliminant ou en empêchant une violation de sécurité, en minimisant les dommages qui peuvent être causés, ou en investiguant et rapportant les risques dans le but d'enclencher des actions correctives.

Fig 1: Gestion du contrôle et Implémentation de la sécurité d'un SI

Les différents types de contrôle

- Contrôle de gestion
- Contrôle opérationnel
- Contrôle technique

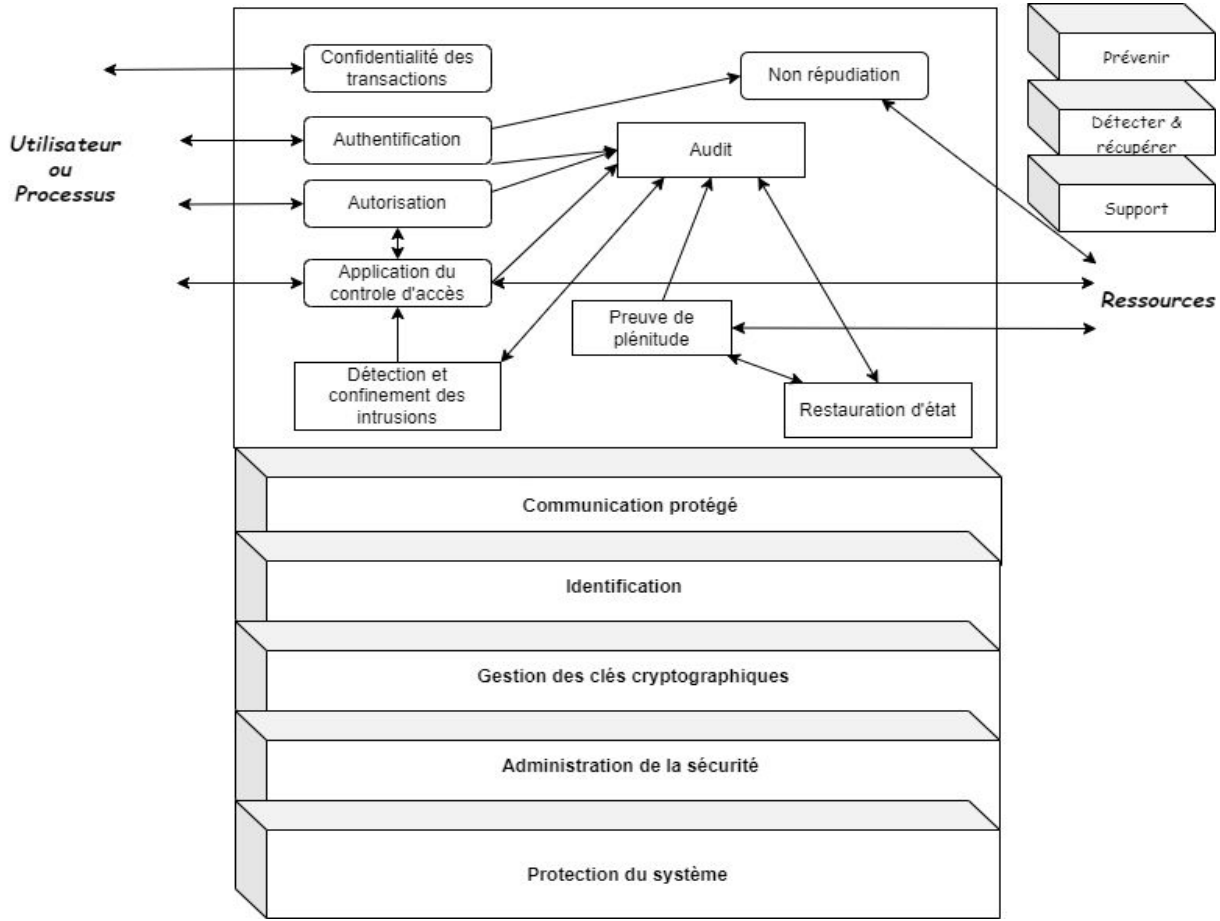


Fig 2: Contrôles techniques de sécurité

Tab1: Contrôle de sécurité selon la norme NIST SP800-53

Types	Familles du contrôle
Contrôles de gestion	Planification
	Gestion des programmes
	Évaluation des risques
	Évaluation de la sécurité et Autorisation
	Acquisition des systèmes et services

Tab1: Contrôle de sécurité selon la norme NIST SP800-53

Types	Familles du contrôle
Contrôles opérationnels	Sensibilisation et formation
	Gestion des configurations
	Plan d'urgence
	Réponses aux incidents
	Maintenance
	Protection des médias

Tab1: Contrôle de sécurité selon la norme NIST SP800-53

Types	Familles du contrôle
Contrôles opérationnels	Sécurité du personnel
	Protection physique et environnementale
	Intégrité du système et de l'information
	Maintenance
	Protection des médias

Tab1: Contrôle de sécurité selon la norme NIST SP800-53

Types	Familles du contrôle
Contrôles Techniques	Contrôle d'accès
	Audit et responsabilité
	Identification et authentification
	Protection du système et des communications
	Protection des médias

Plan de mise en œuvre

Risque (actif/menace)	Attaque de pirate sur le routeur Internet (passerelle)
Niveau de risque	Elevé
Contrôles recommandés	• Désactiver l'accès telnet externe • Utiliser un audit détaillé de l'utilisation des commandes privilégiées • Définir une politique fortes pour les mots de passe administrateur • Définir la stratégie de sauvegarde pour le fichier de configuration du routeur • Définir la politique de contrôle des modifications pour la configuration du routeur
Priorité	Elevée

Plan de mise en œuvre

Contrôles choisis	• Renforcer l'authentification des accès • Installer un logiciel de détection d'intr
Ressources nécessaires	• 3 jours de temps d'administration du réseau informatique pour modifier et vérifier la configuration du routeur, rédiger des politiques • 1 journée de formation pour le personnel d'administration du réseau
Les personnes responsables	• Agbodjan Yves, administrateur principal du système réseau, équipe d'assistance informatique d'entreprise
Date de début et de fin	4 Janvier au 3 Février 2023
Autres commentaires	Nécessite des tests périodiques et un examen de la configuration et de l'utilisation des politiques

Plan de mise en œuvre objectif 11

Objectif 11	Fournir aux utilisateurs, des postes de travail sécurisés pour leurs act
Niveau	
Mesures de sécurité	• Bloquer le partage de fichiers et dossiers locaux • Chiffrer les données sensibles stockées sur les postes de travail • Synchroniser les disques locaux • Installer un anti-virus
Priorité	
Contrôles choisis	

Plan de mise en œuvre objectif 11

Ressources nécessaires	
Niveau	
Les personnes responsables	
Date de début et de fin	
Autres commentaires	

Plan de mise en œuvre objectif 15

Objectif 15	Sécuriser les informations impliquées dans les applications de e-servi
Niveau	
Mesures de sécurité	• Bloquer le partage de fichiers et dossiers locaux • Chiffrer les données sensibles stockées sur les postes de travail • Synchroniser les disques locaux • Installer un anti-virus
Priorité	
Contrôles choisis	

Plan de mise en œuvre objectif 15

Ressources nécessaires	
Niveau	
Les personnes responsables	
Date de début et de fin	
Autres commentaires	