



phosforea

my learning experience



Politique de sécurité

Définir et piloter des indicateurs
et des tableaux de bord SSI

Objectif du cours

Etre capable de rédiger la politique générale de sécurité des systèmes d'information.

Définir et piloter des indicateurs et des tableaux de bord SSI.



Principe général

- A quoi servent les indicateurs et tableaux de bord ?
 - A mesurer une activité, un processus, une mesure ...
 - Faire de la conformité
 - Corriger une situation et prendre (ou aider) des décisions



Références

- Norme ISO27001, article 9.1 : L'organisation doit évaluer les performances de sécurité de l'information, ainsi que l'efficacité du système de gestion de la sécurité de l'information.
 - Quoi ?
 - Quelle méthode (ISO27004) ?
 - Quand ?
 - Qui ?
- Les indicateurs sont aussi soumis à une démarche d'amélioration continue

Conseils de mise en œuvre

- Se focaliser sur des indicateurs compréhensibles par tous, donc orienté métier, donc stratégique
- On peut ponctuellement produire et communiquer des indicateurs pour des objectifs de communication précis (nb de virus)
- Définir une méthodologie
 - la moins chronophage possible
 - avec le moins d'intervenant possible
 - simple dans l'interprétation des indicateurs et la collecte des données
- Définir 1 ou 2 niveaux de granularité maximum

Exercices

- Lister toutes les informations que vous estimez nécessaire dans la formalisation d'une fiche indicateur.



Exercices

- Pour chacune des clauses ou mesures de la norme ISO27001, fournir un exemple d'indicateur
 - §6.1.3 Traitement du risque de sécurité de l'information
 - §7.3 Sensibilisation
 - §9.2 Audit interne
 - A.12.2.1 Il convient de mettre en œuvre des mesures de détection, de prévention et de récupération conjuguées à une sensibilisation des utilisateurs adaptée, pour se protéger contre les logiciels malveillants



Ce module est à présent terminé,
vous pouvez retourner sur votre
tableau de bord.