Appliquer la sécurité R 50

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * appliquer la sécurité de l’information conformément aux politiques et procédures de l’organisation |
| pilote | directeur / responsable sécurité de l’information / chef de projet |
| risques | * ne pas prendre en compte les politiques de l’organisation * ne pas disposer des ressources nécessaires * ne pas prendre en compte les procédures de l’organisation * ne pas passer en revue la sécurité de l’information * ne pas passer en revue les objectifs de sécurité * ne pas passer en revue les mesures de traitement des risques * ne pas passer en revue les processus de sécurité de l’information * ne pas vérifier la conformité du traitement de l’information par rapport aux normes de sécurité applicables * ne pas vérifier la conformité technique des systèmes d’information |
| processus amont | * apprécier les risques * traiter les risques * planifier le SMSI * piloter les processus |
| processus aval | * réaliser la revue de direction * communiquer * satisfaire aux exigences * gérer la continuité de la sécurité de l’information |
| éléments d'entrée | * contexte de l’entreprise * politiques, procédures, processus de l’organisation * normes sécurité * tout risque identifié |
| activités  (sous-processus) | * appliquer la sécurité de l’information dans les politiques et procédures de l’organisation * passer en revue régulièrement :   + le système de sécurité de l’information   + la sécurité de l’information   + les objectifs de sécurité   + les sauvegardes   + les mesures de traitement des risques   + les processus de sécurité de l’information * identifier et traiter les incidents de sécurité de l’information * corriger toute nouvelle vulnérabilité * saisir des opportunités d’amélioration via des audits internes * vérifier la conformité du traitement de l’information par rapport aux normes de sécurité applicables * vérifier la conformité technique des systèmes d’information * évaluer les risques de nouveau * conserver les résultats des revues, des corrections et des évaluations * entreprendre des actions correctives, si nécessaire |
| éléments de sortie | * résultats des audits du SMSI * résultats de la revue de direction * surveillance des mesures de traitement des risques * sensibilisation du personnel |
| ressources | direction, responsables départements, pilotes processus, chefs de projet |
| indicateurs | * non-conformités trouvées * actions mises en place * nouveaux risques identifiés |
| procédures / documents | amélioration continue, communication, planification, audit interne, maîtrise des processus, inspection / liste des risques, plans d'action, fiches processus, rapports d’audit |
| clients | l’ensemble du personnel et des processus, parties intéressées |

Glossaire :

SMSI : système de management de la sécurité de l’information

directeur / responsable sécurité de l’information / chef de projet

* appliquer la sécurité de l’information conformément aux politiques et procédures de l’organisation

appliquer la sécurité / R 50

risques

processus amont

processus aval

* réaliser la revue de direction
* communiquer
* satisfaire aux exigences
* gérer la continuité de la sécurité de l’information
* ne pas prendre en compte les politiques de l’organisation
* ne pas disposer des ressources nécessaires
* ne pas prendre en compte les procédures de l’organisation
* ne pas passer en revue la sécurité de l’information
* ne pas passer en revue les objectifs de sécurité
* ne pas passer en revue les mesures de traitement des risques
* ne pas passer en revue les processus de sécurité de l’information
* ne pas vérifier la conformité du traitement de l’information par rapport aux normes de sécurité applicables
* ne pas vérifier la conformité technique des systèmes d’information
* apprécier les risques
* traiter les risques
* planifier le SMSI
* piloter les processus

activités

éléments d'entrée

éléments de sortie

* résultats des audits du SMSI
* résultats de la revue de direction
* surveillance des mesures de traitement des risques
* sensibilisation du personnel
* appliquer la sécurité de l’information dans les politiques et procédures de l’organisation
* passer en revue régulièrement :
  + le système de sécurité de l’information
  + la sécurité de l’information
  + les objectifs de sécurité
  + les sauvegardes
  + les mesures de traitement des risques
  + les processus de sécurité de l’information
* identifier et traiter les incidents de sécurité de l’information
* corriger toute nouvelle vulnérabilité
* saisir des opportunités d’amélioration via des audits internes
* vérifier la conformité du traitement de l’information par rapport aux normes de sécurité applicables
* vérifier la conformité technique des systèmes d’information
* évaluer les risques de nouveau
* conserver les résultats des revues, des corrections et des évaluations
* entreprendre des actions correctives, si nécessaire
* contexte de l’entreprise
* politiques, procédures, processus de l’organisation
* normes sécurité
* tout risque identifié

ressources

indicateurs

clients

procédures / documents

non-conformités trouvées, actions mises en place, nouveaux risques identifiés

direction, responsables départements, pilotes processus, chefs de projet

amélioration continue, communication, planification, audit interne, maîtrise des processus, inspection / liste des risques, plans d'action, fiches processus, rapports d’audit

l’ensemble du personnel et des processus, parties intéressées