Développer et soutenir la sécurité R 48

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * développer et appliquer les systèmes d’information en incluant les questions de sécurité de l’information * soutenir les systèmes d’information sur les questions de sécurité de l’information |
| pilote | responsable sécurité de l’information |
| risques | * ne pas prendre en compte les questions de sécurité de l’information pendant le développement des systèmes d’information * ne pas soutenir les systèmes d’information sur les questions de sécurité de l’information * ne pas prendre en compte le contexte de l’entreprise * ne pas choisir les options de traitement des risques * ne pas déterminer les mesures de traitement des risques * ne pas mettre en place les mesures de traitement des risques * ne pas élaborer le plan de traitement des risques * ne pas fournir les ressources nécessaires * ne pas attribuer les responsabilités * ne pas déclencher les mesures face aux risques identifiés |
| processus amont | * apprécier les risques * traiter les risques * planifier le SMSI * satisfaire aux exigences de sécurité de l’information |
| processus aval | * appliquer la sécurité de l’information * réaliser la revue de direction * communiquer |
| éléments d'entrée | * cycle de développement des systèmes d’information * politique de développement sécurisé * ressources nécessaires * tout risque identifié |
| activités  (sous-processus) | * établir et appliquer des règles de développement des logiciels * maîtriser les changements au cours du développement par des procédures formelles * vérifier et tester les applications critiques après des changements sur les plateformes opérationnelles * restreindre les modifications des progiciels (*software package*) * documenter les principes d’ingénierie * établir et protéger l’environnement de développement sécurisé qui inclut :   + le personnel   + les processus   + la technologie * surveiller les activités de développement du système externalisé * réaliser des tests de fonctionnalité de sécurité pendant le développement * déterminer des tests de conformité pour tout nouveau système d’information |
| éléments de sortie | * surveillance des processus de développement * sensibilisation du personnel |
| ressources | direction, responsable sécurité de l’information, responsables départements, pilotes processus |
| indicateurs | * risques traités * actions mises en place |
| procédures / documents | amélioration continue, communication, planification, gestion des changements, maîtrise des processus, inspection / liste des risques, plans d'action, fiches processus, demandes de changement, rapports |
| clients | l’ensemble du personnel et des processus, parties intéressées |

Glossaire :

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

* développer et appliquer les systèmes d’information en incluant les questions de sécurité de l’information
* soutenir les systèmes d’information sur les questions de sécurité de l’information

développer et soutenir la sécurité / R 48

responsable sécurité de l’information

risques

processus amont

processus aval

* ne pas prendre en compte les questions de sécurité de l’information pendant le développement des systèmes d’information
* ne pas soutenir les systèmes d’information sur les questions de sécurité de l’information
* ne pas prendre en compte le contexte de l’entreprise
* ne pas choisir les options de traitement des risques
* ne pas déterminer les mesures de traitement des risques
* ne pas mettre en place les mesures de traitement des risques
* ne pas élaborer le plan de traitement des risques
* ne pas fournir les ressources nécessaires
* ne pas attribuer les responsabilités
* ne pas déclencher les mesures face aux risques identifiés
* apprécier les risques
* traiter les risques
* planifier le SMSI
* satisfaire aux exigences de sécurité de l’information
* appliquer la sécurité de l’information
* réaliser la revue de direction
* communiquer

activités

éléments d'entrée

éléments de sortie

* cycle de développement des systèmes d’information
* politique de développement sécurisé
* ressources nécessaires
* tout risque identifié
* surveillance des processus de développement
* sensibilisation du personne
* établir et appliquer des règles de développement des logiciels
* maîtriser les changements au cours du développement par des procédures formelles
* vérifier et tester les applications critiques après des changements sur les plateformes opérationnelles
* restreindre les modifications des progiciels (*software package*)
* documenter les principes d’ingénierie
* établir et protéger l’environnement de développement sécurisé qui inclut :
  + le personnel
  + les processus
  + la technologie
* surveiller les activités de développement du système externalisé
* réaliser des tests de fonctionnalité de sécurité pendant le développement
* déterminer des tests de conformité pour tout nouveau système d’information

ressources

indicateurs

clients

procédures / documents

direction, responsable sécurité de l’information, responsables départements, pilotes processus

risques traités, actions mises en place

amélioration continue, communication, planification, gestion des changements, maîtrise des processus, inspection / liste des risques, plans d'action, fiches processus, demandes de changement, rapports

l’ensemble du personnel et des processus, parties intéressées