Gérer les vulnérabilités R 61

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * prévenir l’exposition aux vulnérabilités techniques * appliquer la politique Gestion des vulnérabilités |
| pilote | responsable sécurité de l’information |
| risques | * ne pas utiliser un inventaire des actifs à jour * ne pas attribuer les responsabilités pour la gestion des vulnérabilités * ne pas avoir identifié les ressources des logiciels utilisés * ne pas inclure dans les contrats avec les fournisseurs les exigences d’un rapport des vulnérabilités * ne pas utiliser des outils d’analyse des vulnérabilités * ne pas conduire des tests d’intrusion * ne pas détecter des vulnérabilités dans ses produits * ne pas recevoir des rapports internes et externes de vulnérabilité * ne pas évaluer les vulnérabilités techniques * ne pas entreprendre des actions sur les vulnérabilités identifiées * utiliser des mises à jour non légitimes |
| processus amont | * apprécier les risques * traiter les risques * auditer * gérer les changements |
| processus aval | * satisfaire aux exigences de la sécurité * tester * appliquer la sécurité * réaliser des actions correctives |
| éléments d'entrée | * plan de traitement des risques * plan de gestion des changements |
| activités  (sous-processus) | * utiliser un inventaire des actifs à jour * attribuer les responsabilités pour la gestion des vulnérabilités * identifier les ressources des logiciels utilisés * inclure dans les contrats avec les fournisseurs les exigences d’un rapport des vulnérabilités * utiliser des outils d’analyse des vulnérabilités * conduire régulièrement des tests d’intrusion * détecter les vulnérabilités dans ses produits * recevoir des rapports internes et externes de vulnérabilité * évaluer les vulnérabilités techniques * entreprendre des actions sur les vulnérabilités identifiées * utiliser des mises à jour légitimes |
| éléments de sortie | * vulnérabilités techniques * rapport d’action corrective * résultats des actions correctives |
| ressources | moyens techniques et informatiques |
| indicateurs | * nombre de vulnérabilités identifiées * nombre d’actions correctives appliquées |
| procédures / documents | activités de surveillance, gestion des vulnérabilités, changements / plan de traitement des risques, plan de gestion des changements, résultats des surveillances et des mesures, vulnérabilités techniques, résultats des revues de sécurité, rapport d’action corrective, résultats des actions correctives |
| clients | auditeurs, ensemble du personnel |

* prévenir l’exposition aux vulnérabilités techniques
* appliquer la politique Gestion des vulnérabilités

responsable sécurité de l’information

gérer les vulnérabilités / R 61

processus amont

risques

processus aval

* satisfaire aux exigences de la sécurité
* tester
* appliquer la sécurité
* réaliser des actions correctives
* apprécier les risques
* traiter les risques
* auditer
* gérer les changements
* ne pas utiliser un inventaire des actifs à jour
* ne pas attribuer les responsabilités pour la gestion des vulnérabilités
* ne pas avoir identifié les ressources des logiciels utilisés
* ne pas inclure dans les contrats avec les fournisseurs les exigences d’un rapport des vulnérabilités
* ne pas utiliser des outils d’analyse des vulnérabilités
* ne pas conduire des tests d’intrusion
* ne pas détecter des vulnérabilités dans ses produits
* ne pas recevoir des rapports internes et externes de vulnérabilité
* ne pas évaluer les vulnérabilités techniques
* ne pas entreprendre des actions sur les vulnérabilités identifiées
* utiliser des mises à jour non légitimes

éléments de sortie

éléments d'entrée

activités

* plan de traitement des risques
* plan de gestion des changements
* utiliser un inventaire des actifs à jour
* attribuer les responsabilités pour la gestion des vulnérabilités
* identifier les ressources des logiciels utilisés
* inclure dans les contrats avec les fournisseurs les exigences d’un rapport des vulnérabilités
* utiliser des outils d’analyse des vulnérabilités
* conduire régulièrement des tests d’intrusion
* détecter les vulnérabilités dans ses produits
* recevoir des rapports internes et externes de vulnérabilité
* évaluer les vulnérabilités techniques
* entreprendre des actions sur les vulnérabilités identifiées
* utiliser des mises à jour légitimes
* vulnérabilités techniques
* rapport d’action corrective
* résultats des actions correctives

procédures / documents

clients

indicateurs

ressources

activités de surveillance, gestion des vulnérabilités, changements / plan de traitement des risques, plan de gestion des changements, résultats des surveillances et des mesures, vulnérabilités techniques, résultats des revues de sécurité, rapport d’action corrective, résultats des actions correctives

auditeurs, ensemble du personnel

nombre de vulnérabilités identifiées, nombre d’actions correctives appliquées

moyens techniques et informatiques