Gérer les incidents R 60

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * planifier et préparer la gestion des incidents * répondre rapidement aux incidents efficacement |
| pilote | responsable sécurité de l’information |
| risques | * ne pas attribuer de responsabilité pour la gestion des incidents * ne pas sensibiliser et former le personnel sur les incidents * ne pas apprécier les risques d’incident (surveillance, détection, analyse) * ne pas traiter les risques d’incident (répondre à l’incident) * ne pas établir et utiliser une méthode de notification des incidents * ne pas catégoriser des événements comme incidents * ne pas savoir limiter la propagation de l’incident * ne pas recueillir et enregistrer des preuves de l’incident * ne pas communiquer et coordonner les actions * ne pas traiter les causes premières * ne pas identifier et gérer les vulnérabilités * ne pas tirer les leçons des incidents |
| processus amont | * planifier le SMSI * apprécier les risques * traiter les risques * dispenser la formation |
| processus aval | * gérer la chaîne TIC * gérer la continuité d’activité * passer en revue la sécurité |
| éléments d'entrée | * plan de traitement des risques * plan de gestion des incidents * événements de sécurité de l’information * plan de continuité d’activité |
| activités  (sous-processus) | * attribuer la responsabilité pour la gestion des incidents * sensibiliser et former le personnel sur les incidents * apprécier les risques d’incident (surveillance, détection, analyse) * traiter les risques d’incident (répondre à l’incident) * établir et utiliser une méthode de notification des incidents * catégoriser des événements comme incidents * limiter la propagation de l’incident * recueillir et enregistrer des preuves de l’incident * communiquer et coordonner les actions * traiter les causes premières * identifier et gérer les vulnérabilités * tirer les leçons des incidents |
| éléments de sortie | * résultats des surveillances et des mesures * registre des incidents * liste de preuves |
| ressources | moyens techniques et informatiques |
| indicateurs | * taux d’incidents détectés * taux d’incidents traités * nombre de causes premières trouvées |
| procédures / documents | chaîne TIC, activités de surveillance, incidents, continuité d’activité / registre des incidents, plan de continuité d’activité, plan de traitement des risques, plan de gestion des incidents, événements de sécurité de l’information, résultats des surveillances et des mesures, liste de preuves |
| clients | ensemble du personnel |

Glossaire :

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

TIC : technologie de l’information et de la communication

* planifier et préparer la gestion des incidents
* répondre rapidement aux incidents efficacement

responsable sécurité de l’information

gérer les incidents / R 60

processus amont

risques

processus aval

* gérer la chaîne TIC
* gérer la continuité d’activité
* passer en revue la sécurité
* planifier le SMSI
* apprécier les risques
* traiter les risques
* dispenser la formation
* ne pas attribuer de responsabilité pour la gestion des incidents
* ne pas sensibiliser et former le personnel sur les incidents
* ne pas apprécier les risques d’incident (surveillance, détection, analyse)
* ne pas traiter les risques d’incident (répondre à l’incident)
* ne pas établir et utiliser une méthode de notification des incidents
* ne pas catégoriser des événements comme incidents
* ne pas savoir limiter la propagation de l’incident
* ne pas recueillir et enregistrer des preuves de l’incident
* ne pas communiquer et coordonner les actions
* ne pas traiter les causes premières
* ne pas identifier et gérer les vulnérabilités
* ne pas tirer les leçons des incidents

éléments de sortie

éléments d'entrée

activités

* attribuer la responsabilité pour la gestion des incidents
* sensibiliser et former le personnel sur les incidents
* apprécier les risques d’incident (surveillance, détection, analyse)
* traiter les risques d’incident (répondre à l’incident)
* établir et utiliser une méthode de notification des incidents
* catégoriser des événements comme incidents
* limiter la propagation de l’incident
* recueillir et enregistrer des preuves de l’incident
* communiquer et coordonner les actions
* traiter les causes premières
* identifier et gérer les vulnérabilités
* tirer les leçons des incidents
* résultats des surveillances et des mesures
* registre des incidents
* liste de preuves
* plan de traitement des risques
* plan de gestion des incidents
* événements de sécurité de l’information
* plan de continuité d’activité

procédures / documents

clients

indicateurs

ressources

ensemble du personnel

chaîne TIC, activités de surveillance, incidents, continuité d’activité / registre des incidents, plan de continuité d’activité, plan de traitement des risques, plan de gestion des incidents, événements de sécurité de l’information, résultats des surveillances et des mesures, liste de preuves

taux d’incidents détectés, taux d’incidents traités, nombre de causes premières

trouvées

moyens techniques et informatiques