Gérer la continuité de sécurité R 49

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * intégrer la continuité de la sécurité de l’information dans la gestion de la continuité d’activité |
| pilote | directeur / responsable sécurité de l’information |
| risques | * ne pas déterminer ses exigences de sécurité de l’information et de continuité de la sécurité de l’information lors d’une crise ou d’un sinistre * ne pas gérer des processus, des procédures et des mesures de continuité de la sécurité de l’information * ne pas vérifier la continuité de la sécurité de l’information * ne pas passer en revues la continuité de la sécurité de l’information * ne pas évaluer la continuité de la sécurité de l’information * ne pas élaborer le plan de traitement des risques * ne pas fournir les ressources nécessaires * ne pas attribuer les responsabilités |
| processus amont | * apprécier les risques * traiter les risques * planifier le SMSI * piloter les processus |
| processus aval | * appliquer la sécurité de l’information * réaliser la revue de direction * communiquer |
| éléments d'entrée | * contexte de l’entreprise * conditions anormales * tout risque identifié d’une situation extraordinaire |
| activités  (sous-processus) | * déterminer ses exigences de sécurité de l’information et de continuité de la sécurité de l’information lors d’une crise ou d’un sinistre * établir, documenter, appliquer et tenir à jour les processus, les procédures et les mesures de continuité de la sécurité de l’information * former et assigner le personnel nécessaire pour gérer la continuité de la sécurité de l’information lors d’une crise ou d’un sinistre * vérifier la continuité de la sécurité de l’information régulièrement * passer en revue et évaluer l’efficacité de la continuité de la sécurité de l’information à l’aide de tests et de simulations * communiquer |
| éléments de sortie | * plan de continuité de la sécurité de l’information * surveillance des mesures de traitement des risques * sensibilisation du personnel |
| ressources | direction, responsables départements, pilotes processus, chefs de projet |
| indicateurs | * risques identifiés * actions mises en place |
| procédures / documents | amélioration continue, communication, planification, maîtrise des processus, inspection / liste des risques, plans de continuité de la sécurité de l’information, fiches processus, rapports |
| clients | l’ensemble du personnel et des processus, parties intéressées |

* intégrer la continuité de la sécurité de l’information dans la gestion de la continuité d’activité

gérer la continuité de sécurité / R 49

directeur / responsable sécurité de l’information

risques

processus amont

processus aval

* apprécier les risques
* traiter les risques
* planifier le SMSI
* piloter les processus
* ne pas déterminer ses exigences de sécurité de l’information et de continuité de la sécurité de l’information lors d’une crise ou d’un sinistre
* ne pas gérer des processus, des procédures et des mesures de continuité de la sécurité de l’information
* ne pas vérifier la continuité de la sécurité de l’information
* ne pas passer en revues la continuité de la sécurité de l’information
* ne pas évaluer la continuité de la sécurité de l’information
* ne pas élaborer le plan de traitement des risques
* ne pas fournir les ressources nécessaires
* ne pas attribuer les responsabilités
* appliquer la sécurité de l’information
* réaliser la revue de direction
* communiquer

activités

éléments d'entrée

éléments de sortie

* plan de continuité de la sécurité de l’information
* surveillance des mesures de traitement des risques
* sensibilisation du personnel
* déterminer ses exigences de sécurité de l’information et de continuité de la sécurité de l’information lors d’une crise ou d’un sinistre
* établir, documenter, appliquer et tenir à jour les processus, les procédures et les mesures de continuité de la sécurité de l’information
* former et assigner le personnel nécessaire pour gérer la continuité de la sécurité de l’information lors d’une crise ou d’un sinistre
* vérifier la continuité de la sécurité de l’information régulièrement
* passer en revue et évaluer l’efficacité de la continuité de la sécurité de l’information à l’aide de tests et de simulations
* communiquer
* contexte de l’entreprise
* conditions anormales
* tout risque identifié d’une situation extraordinaire

ressources

indicateurs

clients

procédures / documents

risques identifiés, actions mises en place

direction, responsables départements, pilotes processus, chefs de projet

amélioration continue, communication, planification, maîtrise des processus, inspection / liste des risques, plans de continuité de la sécurité de l’information, fiches processus, rapports

l’ensemble du personnel et des processus, parties intéressées