Gérer la chaîne TIC R 58

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * maintenir un niveau convenu de sécurité de l’information dans les relations avec les fournisseurs * appliquer la procédure Chaîne TIC |
| pilote | responsable sécurité de l’information |
| risques | * ne pas définir les exigences de sécurité de l’information TIC * ne pas demander aux fournisseurs TIC de retransmettre les exigences de sécurité de l'organisation tout au long de la chaîne TIC * ne pas exiger des fournisseurs TIC de fournir des informations sur les logiciels utilisés * ne pas exiger des fournisseurs TIC de fournir des informations sur les fonctions de sécurité utilisées * ne pas valider les exigences sécurité des produits et service TIC fournis * ne pas identifier et documenter les composants fonctionnels critiques et leur traçabilité * ne pas obtenir d’assurance de fonctionnement des produits et services TIC, de leur origine et du niveau de sécurité requis * ne pas prévoir de composants de rechange |
| processus amont | * planifier le SMSI * apprécier les risques * traiter les risques * maîtriser les processus externalisés * gérer la sécurité des fournisseurs |
| processus aval | * gérer la chaîne TIC * gérer les incidents * gérer les services en nuage * passer en revue la sécurité |
| éléments d'entrée | * liste des parties intéressées * accord fournisseur |
| activités  (sous-processus) | * définir les exigences de sécurité de l’information TIC * demander aux fournisseurs TIC de retransmettre les exigences de sécurité de l'organisation tout au long de la chaîne TIC * exiger des fournisseurs TIC de fournir des informations sur les logiciels utilisés * exiger des fournisseurs TIC de fournir des informations sur les fonctions de sécurité utilisées * valider les exigences sécurité des produits et service TIC fournis * identifier et documenter les composants fonctionnels critiques et leur traçabilité * obtenir l’assurance de fonctionnement des produits et services TIC, de leur origine et du niveau de sécurité requis * prévoir de composants de rechange * gérer la continuité d’activité * gérer les incidents |
| éléments de sortie | * performance fournisseur * sécurité de l’information avec les fournisseurs |
| ressources | moyens techniques et informatiques |
| indicateurs | * taux de fournisseurs sélectionnés * taux d’incidents fournisseurs |
| procédures / documents | transfert de l’information, relations avec les fournisseurs, incidents, continuité d’activité, restrictions d’accès, gestion des vulnérabilités / liste des parties intéressées, accord fournisseur, distribution des accès, performance fournisseur, changements des services des fournisseurs, registre des incidents, plan de continuité d’activité, règles de rupture de contrat, sécurité de l’information avec les fournisseurs, engagement de confidentialité |
| clients | fournisseurs |

Glossaire :

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

TIC : technologie de l’information et de la communication

* maintenir un niveau convenu de sécurité de l’information dans les relations avec les fournisseurs
* appliquer la procédure Chaîne TIC

responsable sécurité de l’information

gérer la chaîne TIC / R 58

processus amont

risques

processus aval

* gérer la chaîne TIC
* gérer les incidents
* gérer les services en nuage
* passer en revue la sécurité
* planifier le SMSI
* apprécier les risques
* traiter les risques
* maîtriser les processus externalisés
* gérer la sécurité des fournisseurs
* ne pas définir les exigences de sécurité de l’information TIC
* ne pas demander aux fournisseurs TIC de retransmettre les exigences de sécurité de l'organisation tout au long de la chaîne TIC
* ne pas exiger des fournisseurs TIC de fournir des informations sur les logiciels utilisés
* ne pas exiger des fournisseurs TIC de fournir des informations sur les fonctions de sécurité utilisées
* ne pas valider les exigences sécurité des produits et service TIC fournis
* ne pas identifier et documenter les composants fonctionnels critiques et leur traçabilité
* ne pas obtenir d’assurance de fonctionnement des produits et services TIC, de leur origine et du niveau de sécurité requis
* ne pas prévoir de composants de rechange

éléments de sortie

éléments d'entrée

activités

* définir les exigences de sécurité de l’information TIC
* demander aux fournisseurs TIC de retransmettre les exigences de sécurité de l'organisation tout au long de la chaîne TIC
* exiger des fournisseurs TIC de fournir des informations sur les logiciels utilisés
* exiger des fournisseurs TIC de fournir des informations sur les fonctions de sécurité utilisées
* valider les exigences sécurité des produits et service TIC fournis
* identifier et documenter les composants fonctionnels critiques et leur traçabilité
* obtenir l’assurance de fonctionnement des produits et services TIC, de leur origine et du niveau de sécurité requis
* prévoir de composants de rechange
* gérer la continuité d’activité
* gérer les incidents
* liste des parties intéressées
* accord fournisseur
* performance fournisseur
* sécurité de l’information avec les fournisseurs

procédures / documents

clients

indicateurs

ressources

transfert de l’information, relations avec les fournisseurs, incidents, continuité d’activité, restrictions d’accès, gestion des vulnérabilités / liste des parties intéressées, accord fournisseur, distribution des accès, performance fournisseur, changements des services des fournisseurs, registre des incidents, plan de continuité d’activité, règles de rupture de contrat, sécurité de l’information avec les fournisseurs, engagement de confidentialité

fournisseurs

taux de fournisseurs sélectionnés, taux d’incidents fournisseurs

moyens techniques et informatiques