Enregistrer et désinscrire R 45

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * maîtriser l’accès des utilisateurs aux systèmes et services d’information * empêcher les accès non autorisés aux systèmes et services d’information |
| pilote | responsable sécurité de l’information |
| risques | * ne pas maîtriser l’accès aux systèmes et services d’information * ne pas empêcher des accès non autorisés aux systèmes et services d’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 * inspecter la sécurité de l’information |
| processus aval | * distribuer les accès des utilisateurs * gérer l’authentification des utilisateurs * appliquer la discipline * appliquer la sécurité de l’information |
| éléments d'entrée | * contexte de l’entreprise * règles d’accès des utilisateurs * tout accès non autorisé identifié |
| activités  (sous-processus) | * attribuer les droits d’accès aux utilisateurs des systèmes et services d’information * permettre à tout utilisateur au moyen d’un identifiant unique de s’enregistrer et de se désinscrire * désinscrire sur le champ les personnes ayant quitté l’organisation * vérifier les droits d’accès des utilisateurs à intervalles réguliers vérifier périodiquement si des identifiants redondants existent et les supprimer * vérifier périodiquement si des identifiants ne sont pas utilisés par des personnes non autorisés |
| éléments de sortie | * règles d’enregistrement et de désinscription * surveillance des mesures de traitement des risques * sensibilisation du personnel |
| ressources | responsable sécurité de l’information, systèmes d’information, logiciels |
| indicateurs | * accès non autorisés découverts * risques traités * actions mises en place |
| procédures / documents | amélioration continue, communication, planification, maîtrise des processus, inspection / liste des risques, plans d'action, fiches processus, rapports |
| clients | l’ensemble du personnel et des processus, parties intéressées |

* maîtriser l’accès des utilisateurs aux systèmes et services d’information
* empêcher les accès non autorisés aux systèmes et services d’information

responsable sécurité de l’information

enregistrer et désinscrire / R 45

titre / codification

finalité

pilote

risques

processus amont

processus aval

* distribuer les accès des utilisateurs
* gérer l’authentification des utilisateurs
* appliquer la discipline
* appliquer la sécurité de l’information
* apprécier les risques
* traiter les risques
* inspecter la sécurité de l’information
* ne pas maîtriser l’accès aux systèmes et services d’information
* ne pas empêcher des accès non autorisés aux systèmes et services d’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

éléments de sortie

activités

éléments d'entrée

* règles d’enregistrement et de désinscription
* surveillance des mesures de traitement des risques
* sensibilisation du personnel
* attribuer les droits d’accès aux utilisateurs des systèmes et services d’information
* permettre à tout utilisateur au moyen d’un identifiant unique de s’enregistrer et de se désinscrire
* désinscrire sur le champ les personnes ayant quitté l’organisation
* vérifier les droits d’accès des utilisateurs à intervalles réguliers vérifier périodiquement si des identifiants redondants existent et les supprimer
* vérifier périodiquement si des identifiants ne sont pas utilisés par des personnes non autorisés
* contexte de l’entreprise
* règles d’accès des utilisateurs
* tout accès non autorisé identifié

clients

procédures / documents

indicateurs

ressources

accès non autorisés découverts, risques traités, actions mises en place

amélioration continue, communication, planification, maîtrise des processus, inspection / liste des risques, plans d'action, fiches processus, rapports

responsable sécurité de l’information, systèmes d’information, logiciels

l’ensemble du personnel et des processus, parties intéressées