Distribuer les accès R 46

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * pouvoir attribuer les droits d’accès aux utilisateurs des systèmes et services d’information * pouvoir retirer les droits d’accès aux utilisateurs des systèmes et services d’information * sécuriser les décisions liées aux droits d’accès |
| pilote | responsable sécurité de l’information |
| risques | * ne pas maîtriser l’attribution des droits d’accès des utilisateurs aux systèmes et services d’information * ne pas maîtriser le retrait des droits d’accès des utilisateurs aux systèmes et services d’information * permettre des accès non autorisés aux systèmes et services d’information * 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 attribuer les responsabilités * ne pas déclencher les mesures face aux risques identifiés |
| processus amont | * apprécier les risques * traiter les risques * enregistrer et désinscrire les utilisateurs * développer la politique |
| processus aval | * gérer l’authentification des utilisateurs * appliquer la discipline * appliquer la sécurité de l’information |
| éléments d'entrée | * contexte de l’entreprise * règles de distribution des accès des utilisateurs * règles de retrait des accès des utilisateurs |
| activités  (sous-processus) | * valider la liste des utilisateurs et groupes d’utilisateurs * attribuer les droits d’accès aux utilisateurs des systèmes et services d’information :   + avec autorisation de la direction, si nécessaire   + après la validation des procédures d'autorisation * vérifier que le niveau d’accès attribué est conforme aux exigences métier et aux responsabilités cloisonnées * conserver l’historique des droits d'accès accordés à un identifiant * adapter les droits d'accès des utilisateurs qui ont changé de fonction * retirer sur le champ les droits d’accès aux utilisateurs ayant quitté l’organisation * vérifier les droits d’attribution des accès des utilisateurs à intervalles réguliers * inclure des clauses dans les contrats de travail qui précisent les sanctions en cas de tentative d'accès non autorisé |
| éléments de sortie | * règles d’attribution et de retrait des droits d’accès * surveillance des mesures de traitement des risques * sensibilisation du personnel |
| ressources | responsable sécurité de l’information, systèmes d’information, logiciels |
| indicateurs | * droits d’accès non autorisés découverts * droits d’accès retirés * 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 |

finalité

titre / codification

pilote

* pouvoir attribuer les droits d’accès aux utilisateurs des systèmes et services d’information
* pouvoir retirer les droits d’accès aux utilisateurs des systèmes et services d’information
* sécuriser les décisions liées aux droits d’accès

distribuer les accès / R 46

responsable sécurité de l’information

risques

processus amont

processus aval

* ne pas maîtriser l’attribution des droits d’accès des utilisateurs aux systèmes et services d’information
* ne pas maîtriser le retrait des droits d’accès des utilisateurs aux systèmes et services d’information
* permettre des accès non autorisés aux systèmes et services d’information
* 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 attribuer les responsabilités
* ne pas déclencher les mesures face aux risques identifiés
* apprécier les risques
* traiter les risques
* enregistrer et désinscrire les utilisateurs
* développer la politique
* gérer l’authentification des utilisateurs
* appliquer la discipline
* appliquer la sécurité de l’information

activités

éléments d'entrée

éléments de sortie

* valider la liste des utilisateurs et groupes d’utilisateurs
* attribuer les droits d’accès aux utilisateurs des systèmes et services d’information :
  + avec autorisation de la direction, si nécessaire
  + après la validation des procédures d'autorisation
* vérifier que le niveau d’accès attribué est conforme aux exigences métier et aux responsabilités cloisonnées
* conserver l’historique des droits d'accès accordés à un identifiant
* adapter les droits d'accès des utilisateurs qui ont changé de fonction
* retirer sur le champ les droits d’accès aux utilisateurs ayant quitté l’organisation
* vérifier les droits d’attribution des accès des utilisateurs à intervalles réguliers
* inclure des clauses dans les contrats de travail qui précisent les sanctions en cas de tentative d'accès non autorisé
* contexte de l’entreprise
* règles de distribution des accès des utilisateurs
* règles de retrait des accès des utilisateurs
* règles d’attribution et de retrait des droits d’accès
* surveillance des mesures de traitement des risques
* sensibilisation du personnel

clients

procédures / documents

indicateurs

ressources

droits d’accès non autorisés découverts, droits d’accès retirés, 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