Gérer l’authentification R 47

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * attribuer à chaque utilisateur un identifiant unique * authentifier l’utilisateur (vérifier son identité) par un moyen sécurisé (comme mot de passe) * protéger l’authentification des utilisateurs |
| pilote | responsable sécurité de l’information |
| risques | * ne pas maîtriser les informations secrètes d’authentification des utilisateurs * permettre 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 * enregistrer et désinscrire les utilisateurs * distribuer les accès des utilisateurs |
| processus aval | * développer et assister la sécurité * appliquer la discipline * appliquer la sécurité de l’information |
| éléments d'entrée | * contexte de l’entreprise * règles d’accès des utilisateurs * règles d’authentification des utilisateurs |
| activités  (sous-processus) | * définir les règles pour les mots de passe :   + choix   + dimension   + restrictions   + renouvellement   + sanctions disciplinaires * attribuer des informations secrètes d’authentification à chaque utilisateur des systèmes et services d’information par défaut * demander aux utilisateurs d’accuser réception des informations d'authentification secrètes * faire signer un engagement d’utilisateur sur la confidentialité des informations d'authentification secrètes * demander à tout utilisateur de changer ses informations secrètes d’authentification données par défaut dès la première utilisation * vérifier les droits d’accès des utilisateurs à intervalles réguliers * supprimer les droits d’accès quand cela est nécessaire * attribuer des informations d'authentification secrètes temporaires à une seule personne, si nécessaire |
| éléments de sortie | * règles d’authentification et de désinscription * surveillance des mesures de traitement des risques * sensibilisation du personnel |
| ressources | responsable sécurité de l’information, systèmes d’information, logiciels |
| indicateurs | * incidents d’authentification * 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, engagement d’utilisateur |
| clients | l’ensemble du personnel et des processus, parties intéressées |

* attribuer à chaque utilisateur un identifiant unique
* authentifier l’utilisateur (vérifier son identité) par un moyen sécurisé (comme mot de passe)
* protéger l’authentification des utilisateurs

gérer l’authentification / R 47

responsable sécurité de l’information

risques

processus amont

processus aval

* apprécier les risques
* traiter les risques
* enregistrer et désinscrire les utilisateurs
* distribuer les accès des utilisateurs
* ne pas maîtriser les informations secrètes d’authentification des utilisateurs
* permettre 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
* développer et assister la sécurité
* appliquer la discipline
* appliquer la sécurité de l’information

activités

éléments d'entrée

éléments de sortie

* définir les règles pour les mots de passe :
  + choix
  + dimension
  + restrictions
  + renouvellement
  + sanctions disciplinaires
* attribuer des informations secrètes d’authentification à chaque utilisateur des systèmes et services d’information par défaut
* demander aux utilisateurs d’accuser réception des informations d'authentification secrètes
* faire signer unengagement d’utilisateursur la **co**nfidentialité des informations d'authentification secrètes
* demander à tout utilisateur de changer ses informations secrètes d’authentification données par défaut dès la première utilisation
* vérifier les droits d’accès des utilisateurs à intervalles réguliers
* supprimer les droits d’accès quand cela est nécessaire
* attribuer des informations d'authentification secrètes temporaires à une seule personne, si nécessaire
* règles d’authentification et de désinscription
* surveillance des mesures de traitement des risques
* sensibilisation du personnel
* contexte de l’entreprise
* règles d’accès des utilisateurs
* règles d’authentification des utilisateurs

clients

procédures / documents

indicateurs

ressources

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

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

incidents d’authentification, risques traités, actions mises en place

l’ensemble du personnel et des processus, parties intéressées