Utiliser la cryptographie R 64

|  |  |
| --- | --- |
| type | processus de réalisation |
| finalité | * assurer une utilisation appropriée et efficace de la cryptographie pour protéger la confidentialité, l'authenticité ou l'intégrité de l’information conformément aux exigences de l’organisation et de sécurité de l'information * tenir compte des exigences légales, statutaires, réglementaires et contractuelles liées à la cryptographie * respecter la politique Utilisation de la cryptographie |
| pilote | responsable sécurité de l’information |
| risques | * ne pas définir et appliquer les règles cryptographiques * ne pas tenir compte des exigences légales, statutaires, réglementaires et contractuelles liées à la cryptographie * ne pas respecter la politique Utilisation de la cryptographie * le niveau de protection n’est pas adéquat à l’appréciation du risque * ne pas crypter les échanges de données sensibles sur les réseaux * ne pas gérer de manière appropriée et efficace les clés cryptographiques * ne pas attribuer les responsabilités pour la gestion de la cryptographie * ne pas inclure des clauses sur la fiabilité et le temps de réponse des fournisseurs |
| processus amont | * apprécier les risques * traiter les risques * classification de l’information * sécurité des réseaux |
| processus aval | * satisfaire aux exigences de la sécurité * appliquer la sécurité * administrer les réseaux |
| éléments d'entrée | * inventaire des actifs * plan de traitement des risques * clés cryptographiques |
| activités  (sous-processus) | * définir et appliquer les règles cryptographiques * tenir compte des exigences légales, statutaires, réglementaires et contractuelles liées à la cryptographie * respecter la politique Utilisation de la cryptographie * assurer un niveau de protection adéquat à l’appréciation du risque * crypter les échanges de données sensibles sur les réseaux * gérer de manière appropriée et efficace les clés cryptographiques (générer, stocker, archiver, récupérer, distribuer, retirer et détruire) * attribuer les responsabilités pour la gestion de la cryptographie * inclure des clauses sur la fiabilité et le temps de réponse des fournisseurs |
| éléments de sortie | * sortie des actifs * demande de changement * suppression de l’information |
| ressources | moyens techniques et informatiques |
| indicateurs | * taux de données cryptées * clés cryptographiques utilisées |
| procédures / documents | utilisation de la cryptographie, traitement de l’information, classification de l’information, transfert de l’information, terminaux utilisateurs, relations avec les fournisseurs, supports de stockage, changements / plan de traitement des risques, plan de gestion des changements, demande de changement, résultats des revues de sécurité, sécurité des appareils mobiles, clés cryptographiques, plan de classification, données de transfert, mot de passe, sécurité de l’information avec les fournisseurs |
| clients | ensemble du personnel |

* assurer une utilisation appropriée et efficace de la cryptographie pour protéger la confidentialité, l'authenticité ou l'intégrité de l’information conformément aux exigences de l’organisation et de sécurité de l'information
* tenir compte des exigences légales, statutaires, réglementaires et contractuelles liées à la cryptographie
* respecter la politique Utilisation de la cryptographie

responsable sécurité de l’information

utiliser la cryptographie / R 64

risques

processus aval

processus amont

* satisfaire aux exigences de la sécurité
* appliquer la sécurité
* administrer les réseaux
* apprécier les risques
* traiter les risques
* classification de l’information
* sécurité des réseaux
* ne pas définir et appliquer les règles cryptographiques
* ne pas tenir compte des exigences légales, statutaires, réglementaires et contractuelles liées à la cryptographie
* ne pas respecter la politique Utilisation de la cryptographie
* le niveau de protection n’est pas adéquat à l’appréciation du risque
* ne pas crypter les échanges de données sensibles sur les réseaux
* ne pas gérer de manière appropriée et efficace les clés cryptographiques
* ne pas attribuer les responsabilités pour la gestion de la cryptographie
* ne pas inclure des clauses sur la fiabilité et le temps de réponse des fournisseurs

activités

éléments de sortie

éléments d'entrée

* définir et appliquer les règles cryptographiques
* tenir compte des exigences légales, statutaires, réglementaires et contractuelles liées à la cryptographie
* respecter la politique Utilisation de la cryptographie
* assurer un niveau de protection adéquat à l’appréciation du risque
* crypter les échanges de données sensibles sur les réseaux
* gérer de manière appropriée et efficace les clés cryptographiques (générer, stocker, archiver, récupérer, distribuer, retirer et détruire)
* attribuer les responsabilités pour la gestion de la cryptographie
* inclure des clauses sur la fiabilité et le temps de réponse des fournisseurs
* sortie des actifs
* demande de changement
* suppression de l’information
* inventaire des actifs
* plan de traitement des risques
* clés crypto-graphiques

procédures / documents

clients

indicateurs

ressources

utilisation de la cryptographie, traitement de l’information, classification de l’information, transfert de l’information, terminaux utilisateurs, relations avec les fournisseurs, supports de stockage, changements / plan de traitement des risques, plan de gestion des changements, demande de changement, résultats des revues de sécurité, sécurité des appareils mobiles, clés cryptographiques, plan de classification, données de transfert, mot de passe, sécurité de l’information avec les fournisseurs

taux de données cryptées, clés cryptographiques utilisées

ensemble du personnel

moyens techniques et informatiques