

Sécurité des Systèmes d 'Information
Une politique simple pour parler à
la Direction Générale
De la théorie à la pratique

Sommaire

- Fondements d'une politique de sécurité
- Les 9 axes parallèles d'une politique de sécurité
- Reporting, ROI

Principe de base de la sécurité

Démarche globale de maîtrise des risques informatiques

```
graph TD; A[Démarche globale de maîtrise des risques informatiques] --> B[Minimiser les pertes financières, de savoir-faire et d'image]; A --> C[Réduire les risques technologiques et informationnel à un niveau acceptable pour l'entreprise]; A --> D[Permettre un usage efficace et économique des technologies];
```

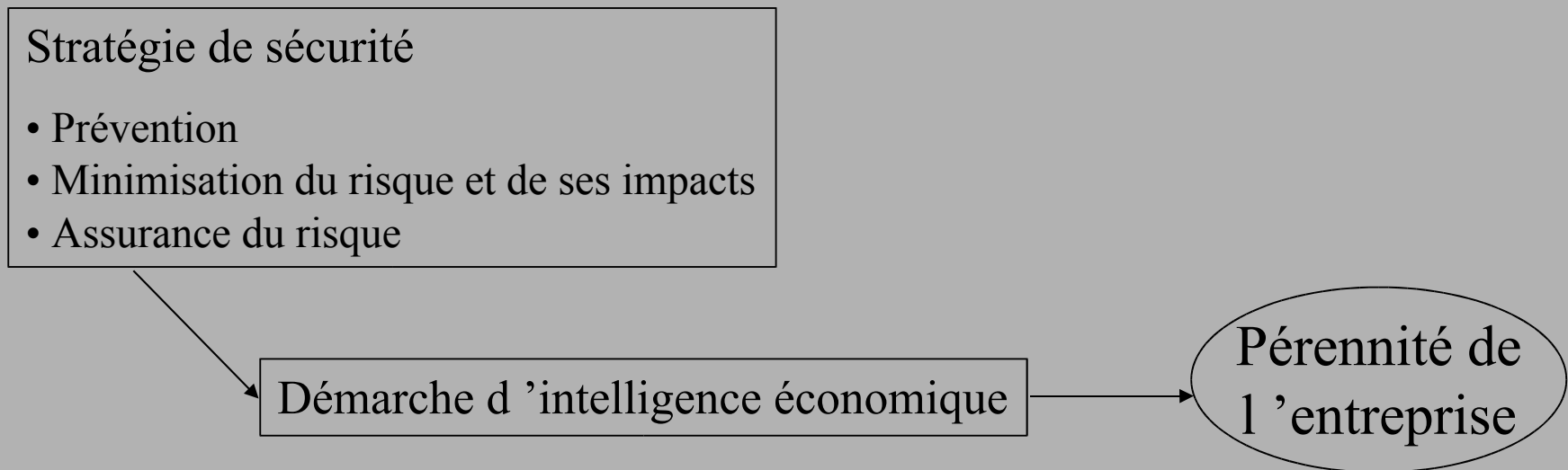
Minimiser les pertes financières, de savoir-faire et d'image

Réduire les risques technologiques et informationnel à un niveau acceptable pour l'entreprise

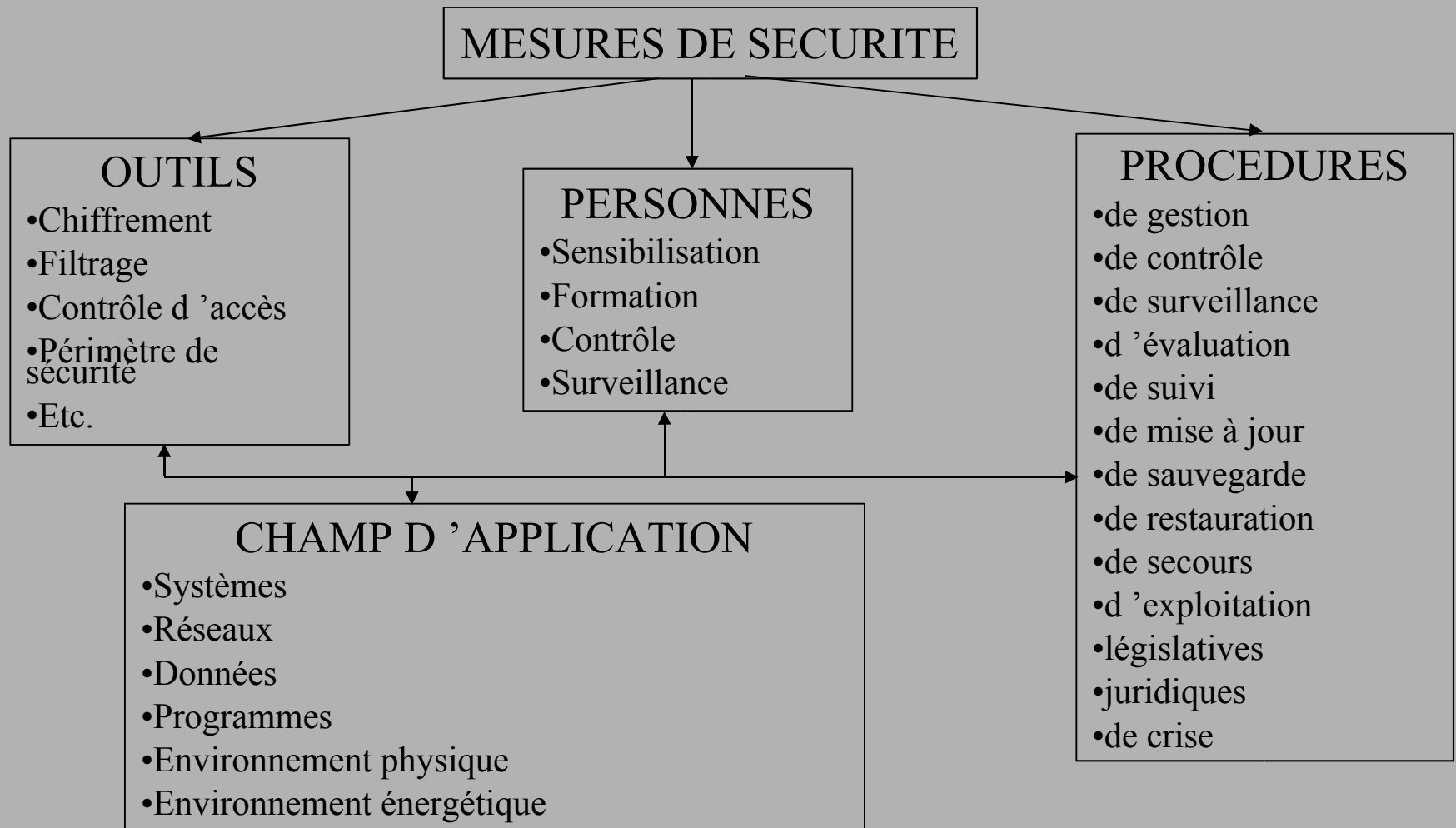
Permettre un usage efficace et économique des technologies

Objectif central de la sécurité

La sécurité ne permet pas directement de gagner de l'argent mais évite d'en perdre. Ce n'est rien d'autre qu'une stratégie préventive qui s'inscrit dans une approche d'intelligence économique.



Complémentarité des procédures, outils et personnes



Les conditions du succès de la démarche sécurité

- Une volonté directoriale
- Une politique de sécurité simple, précise, compréhensible et applicable
- La publication de cette politique de sécurité
- Une gestion centralisée de la sécurité et une certaine automatisation des processus de sécurité
- Un niveau de confiance déterminé des personnes, des systèmes
- Du personnel sensibilisé et formé à la sécurité, possédant une haute valeur morale
- Des procédures d 'enregistrement, de surveillance, d 'audit, d 'organisation
- Une certaine éthique et un respect des contraintes légales

Question simples mais réponses précises

- Quelles sont les « valeurs » de la Société ?
- Quel est leur niveau de sensibilité ou de criticité ?
- De qui, de quoi doit-on se protéger ?
- Quels sont les risques réellement encourus ?
- Ces risques sont-ils supportables et jusqu 'à quel niveau ?
- Quel est le niveau actuel de sécurité ?
- Quel est le niveau de sécurité que l 'on souhaite atteindre ?
- Comment passer du niveau actuel au niveau désiré ?
- Quelles sont les contraintes effectives ?
- Quels sont les moyens disponibles ?

Une démarche en 3 phases

1

Un projet d'entreprise

- Définir une politique de sécurité
- Attribuer des responsabilités à des personnes compétentes possédant l'autorité et les moyens nécessaires
- Identifier les composants à sécuriser
- Déterminer les enjeux (importance du composant)
- Définir les menaces potentielles affectant le composant
- Estimer les failles de sécurité du système en place

2

Quantification et réalisation des mesures sécuritaires

- Proposer des recommandations chiffrées
- Mettre en place des outils, mécanismes, procédures permettant de déployer les règles de sécurité

3

Gérer le quotidien

- Tester les mesures implantées
- Exploiter et administrer les outils déployés
- Auditer, valider et adapter les mesures en place

Politique de sécurité : 9 axes complémentaires

- Politique générale de sécurité
- Traitement et protection de l 'information
- Sensibilisation
- Communication et reporting
- Sécurité physique
- Conformité aux lois et règles internes
- Sécurité des infrastructures réseau & télécom
- Sécurité des applications
- Continuité de l 'activité

Présentation des 9 modules de la Politique de Sécurité

« Toute musique qui ne peint rien
n 'est que du bruit »

Jean le Rond d 'Alembert



Politique générale de sécurité

Module n°1

- Organisation du Programme de Sécurité
- Définition et attribution des responsabilités
 - La toile du programme de sécurité d'entreprise. Notion de filets.
- Une Charte de Sécurité d'entreprise
 - Pourquoi et pour qui ? Qui en sont les acteurs et les rédacteurs ? Exemples de chartes d'entreprise. Législation en vigueur.
- Evaluation du niveau de sécurité
 - Méthode SLAM (Security Level Analysis Method). Les 300 questions de SLAM. Le rapport d'évaluation SLAM. La mesure annuelle.
- Les standards de sécurité d'entreprise
 - Description des standards.
 - Qualification des standards.

Traitement et protection de l'information

Module n°2

- Notion de propriété / Délégation de propriété
- Classification de l'information
 - Les degrés : publique, interne, confidentielle, secrète. Les outils de classification. Les analyses de risque. Le suivi des risques.
- Protection de l'information
 - Le chiffrement des données locales. Notion de cryptographie. Circulation sécurisée de l'information.
- Disponibilité de l'information
 - Sauvegardes et restauration. Les méthodes actuelles (clustering, mirroring, SAN...).
- Confidentialité de l'information
 - Processus d'administration des droits. Authentification simple et forte.

Sensibilisation

Module n°3

- Sensibiliser le personnel = Faire accepter les contraintes
- Diffusion du programme de sécurité
- Le rôle des Ressources Humaines
- Le rôle des Comités d'Entreprise et des Partenaires Sociaux
- Les outils de diffusion du programme de sécurité.
- Le programme de sensibilisation des collaborateurs
 - Le contrat de travail. L'entretien annuel d'appréciation. Les journaux d'information. Les sessions de formation internes et externes. Le parcours d'intégration à l'entreprise.

Communication et reporting

Module n°4

- La prise en compte des spécificités géographiques et géopolitiques
- Les synergies internes
 - Communiquer le programme de sécurité. L'Intranet d'Entreprise.
- Le reporting DG - Datawarehouse
 - L'information continue des décideurs. La « vente » du programme de sécurité au payeur.
- La communication inter-correspondants
 - Synergie entre les Correspondants. Animation des réseaux de Correspondants.

Sécurité physique

Module n°5

- Sécurité des infrastructures physiques
 - L'anti-incendie. L'anti-intrusion. La gestion des composants énergétiques.
- Sécurité des matériels
 - Les onduleurs. Les zones et périmètres de sécurité. La gestion physique des sauvegardes. L'externalisation.
- Sécurité des personnes
- Le Comité de Coordination Sécurité des SI / Sécurité des infrastructures physiques
 - Rôle et prérogatives du Comité. Composition du Comité.

Conformité aux lois et règles internes

Module n°6

- La veille juridique
- Implication de la Direction Juridique
- Implication des Partenaires Sociaux et des Comités d'Entreprise
- Le règlement intérieur.
 - Mise en accord ou révision.
- Le flou juridique actuel
 - Jurisprudence sur l'utilisation des systèmes d'information. Loi «informatique et libertés ». Loi Godfrain. Législation internationale.

Sécurité des infrastructures réseaux et télécoms

Module n°7 (1)

- Infrastructure Réseaux et Télécoms : état de l'art
- Les protocoles réseau : TCP/IP, SMTP, SNMP, HTTP, HTTPS, UDP
- Failles de sécurité des protocoles de communication réseau
- Le réseau Internet
 - Historique organisationnel et technique
 - Fonctionnement technique
 - Relations avec les réseaux privés
 - Failles de sécurité du réseau Internet
 - Banditisme et hacking
 - Phreaking, Carding, Cracking...
 - Le monde « underground »
 - La riposte internationale

Sécurité des infrastructures réseaux et télécoms

Module n°7 (2)

- Les attaques
 - Les attaques par protocole (IP Spoofing, Sinflooding...)
 - Les intrusions
 - Les scans réseau
 - Les virus, les chevaux de Troie, les bombes logiques
 - Description pratique : composition algorithmique du virus
 - Attaque par cheval de Troie
- Politique antivirus d'entreprise
- Firewall
 - Description fonctionnelle
 - Schéma d'architecture de Firewall – Étude
 - Paramétrage et maintenance du Firewall
 - Produits du marché

Sécurité des infrastructures réseaux et télécoms

Module n°7 (3)

- Les sondes de détection d'intrusion
 - Description fonctionnelle
 - Analyse technique
 - Intégration au schéma d'architecture sécurité
 - Produits du marché
- Sécurité des composants réseau
 - Routeurs – Routeurs filtrants
 - Oebs – Lignes RNIS, LS, CFT
- Sécurité des machines serveurs
 - Les zones serveurs
 - Les failles de sécurité standards
 - Approche UNIX – Approche NT – Approche NOVELL

Sécurité des infrastructures réseaux et télécoms

Module n°7 (4)

- Sécurité des machines serveurs
 - Les serveurs WEB
 - Architecture avec DMZ
 - Attaques sur serveurs WEB – Déni de service
- Sécurité des postes de travail
 - Les droits et privilèges utilisateurs
 - La politique de gestion de parc
 - Les standards de malveillance interne
 - Le chiffrement des données locales
 - Le firewall personnel
 - Relation avec la charte de déontologie

Sécurité des infrastructures réseaux et télécoms

Module n°7 (5)

- Sécurité des communications
 - VPN (Virtual Private Network) – Étude technique et fonctionnelle
 - Cryptographie – Systèmes à clés publiques – Systèmes à clés privés
 - Certification et non répudiation
- Administration et organisation du réseau
 - Attribution et gestion des droits d'accès aux systèmes
 - Attribution et gestion des droits d'accès aux applications
 - Monitoring et analyses des logs générées
- Authentification forte
 - Les cartes à puce
 - La biométrie – Évolution de la biotechnologie

Sécurité des applications

Module n°8

- Analyses de risques du parc applicatif
- Schéma du parc applicatif
- Évaluation du niveau de sécurité des applications
 - Méthode d'évaluation
 - Classification
 - Relations propriétaires d'application
- Développement et maintenance des applications
 - Normes de développement
 - Ergonomie des développements
- Intégration des applications externes
 - Analyse de risque. Analyse d'intégration
 - Mise à jour du schéma applicatif

Continuité d'activité

Module n°9 (1)

- Le secours informatique
- La continuité d'activité des métiers
 - présentation générale
 - gestion, maintenance et audit du plan de continuité d'activité
 - organisation du plan de continuité d'activité
 - plan de sauvegarde et d'archivage
 - les tests
 - gestion de la crise
 - gestion de la communication
 - mesures conservatoires
 - mesures d'urgence

Continuité d'activité

Module n°9 (2)

- La continuité d'activité des métiers
 - continuité des métiers
 - logistique de repli
 - bascule serveurs
 - reprise technique
 - reprise fonctionnelle
 - remise à niveau du site sinistré
 - exploitation et fonctionnement en mode secours
 - retour
 - gestion sociale
 - trésorerie de crise

Sécurité : photographie

Champ d'application d'un programme de sécurité

- Toutes les divisions de l'entreprise, entités et lignes métiers doivent appliquer le programme de sécurité.
- Tous les traitements d'information de l'entreprise, sans exception, doivent se conformer aux exigences du programme de sécurité.
- Les partenaires, les fournisseurs et les prestataires de service doivent se conformer aux règles du programme de sécurité.
- Les transactions avec les sociétés externes et les organisations que l'entreprise sert ou qui servent l'entreprise doivent suivre les principes du programme de sécurité.

Obligations générales

- Tout employé ou collaborateur de l'entreprise doit se conformer aux exigences du programme de sécurité et aux standards et procédures qui en résultent.
- Aucune exception n'est autorisée sans une implication et une justification motivée du Management.
- Un audit interne régulier est responsable de vérifier régulièrement l'adéquation des modes de fonctionnement avec le programme de sécurité de l'entreprise.

Sécurité des informations du Groupe : exigences générales.

- La confidentialité de l'information est suffisamment assurée.
- La confiance en l'intégrité de l'information est convenablement assurée.
- L'information est disponible lorsque les métiers en nécessitent l'usage.
- La non répudiation entre l'entreprise et ses interlocuteurs est assurée.
- Toutes les obligations légales, statutaires, contractuelles et régulatrices sont maîtrisées et assurées.

Sécurité des informations : exigences générales.

- Les utilisateurs du système d'information de l'entreprise doivent être identifiés et l'utilisation qu'ils font des ressources validée et contrôlée.
- L'accès aux ressources de l'entreprise doit être basé sur les besoins exacts du métier de chaque utilisateur.
- Ces accès doivent être décrits et validés par les propriétaires d'information.

Responsabilités

- Direction Générale
- Responsables Métiers
- Propriétaire d'information
- Gestionnaire de ressources
- Utilisateur
- Responsable Sécurité des Systèmes d'Information
- Correspondants Sécurité Entités (CSE)
- Correspondant Sécurité Technique (CST)
- Correspondant Sécurité Métier (CSM)

Direction Générale

- La Direction Générale est le moteur du Programme de Sécurité
- Son soutien est essentiel pour le déploiement du programme de sécurité
- La Direction Générale valide la politique de sécurité, le programme de sécurité et les projets induits
- La Direction Générale est informée régulièrement des avancées du programme
- La Direction Générale est informée de toute atteinte à la sécurité des valeurs de l 'entreprise

Responsables Métiers

- Les Responsables Métiers ont pleinement connaissance du programme de sécurité
- Les Responsables Métiers mettent leur position hiérarchique au service du programme de sécurité
- Les Responsables Métiers sont garants de l 'implémentation du programme de sécurité dans leurs aires de responsabilité
- Le RSSI doit fournir aux Responsables Métiers les éléments techniques ou de réflexion nécessaires à la prise en compte de la sécurité dans leurs métiers

Propriétaire d'information

Le Propriétaire d'information doit s'assurer des points suivants :

- Une analyse de risque liée aux ressources dont il est propriétaire est conduite et son résultat est cohérent.
- Des contrôles sont appliqués pour vérifier l'adéquation avec les exigences de sécurité définies par le programme (standards, préconisations suite à l'analyse de risque...).
- Les ressources sont régulièrement passées en revue pour vérifier leur conformité aux exigences de sécurité.
- L'accès aux ressources est limité aux exigences du métier des utilisateurs.
- Les droits d'accès aux ressources sont définis, justifiés et documentés. Ils sont régulièrement vérifiés et validés.

Gestionnaire de ressource

- Les ressources appartenant à des Propriétaires sont administrées, modifiées, gérées par des “Gestionnaires”.
- Le Gestionnaire de ressources crée, modifie, traite ou utilise les ressources.
- Chaque Gestionnaire doit être en relation avec son CST ou son CSM.
- Chaque Gestionnaire doit rendre compte des évolutions des ressources à leur Propriétaire.
- Le Gestionnaire de ressources doit travailler avec son CST ou son CSM sur les points suivants : une analyse de risque est conduite pour chaque nouvelle ressource, des contrôles sont implémentés suivant les préconisations du Propriétaire ou de la politique générale de sécurité, le Propriétaire est tenu au courant de l'évolution des risques et des éventuels incidents qui surviennent.

Utilisateur

- Un utilisateur est un employé, un contractuel, un prestataire et plus généralement toute personne utilisant une ressource.
- L'utilisateur doit se conformer aux règles de sécurité, quelle que soit son action (création, modification, traitement, utilisation d'information ou de ressources).
- L'utilisateur doit être sensibilisé et formé aux règles de sécurité. Il doit avoir connaissance de ses droits et devoirs.
- L'utilisateur doit remonter vers sa hiérarchie ou son Responsable Sécurité toute forme d'atteinte à la politique de sécurité (dysfonctionnement des systèmes, virus...).

Responsable Sécurité des SI

- Le Service Sécurité est responsable de la sécurisation des processus et des transactions de l'entreprise, de la définition de standards pertinents et de l'application d'un programme de sécurité évolutif.
- Le Service Sécurité est responsable du programme de sensibilisation, de l'explication des actions de sécurité et de la distribution des responsabilités, comme défini dans le programme de sécurité de l'entreprise.

Responsable Sécurité des SI

Le Service Sécurité a les responsabilités suivantes :

- Evaluer et gérer les risques informatiques, physiques et plus généralement susceptibles d'intenter au patrimoine informationnel.
- Rédiger et diriger un programme de sécurité pertinent dans le but d'implémenter une politique de sécurité définie.
- Diriger un programme de sensibilisation et d'information auprès du personnel.
- Acquérir et organiser le déploiement d'outils de sécurité modernes et répondant aux exigences du programme.
- Assurer une veille technologique constante dans le domaine de la sécurité.
- Effectuer un reporting régulier sur les évolutions du programme sécurité à la Direction Générale.

CST

Correspondant

Sécurité

Technique



Rôle du CST

- Promouvoir le programme de sécurité dans son aire de responsabilité.
- S'assurer de la mise en œuvre des orientations de sécurité.
- Collaborer activement avec le RSSI.

- Le CST participe aux Comités de Suivi de l'ensemble des projets en cours dans son aire de responsabilité.
- Le CST conseille le Service Sécurité sur les aspects techniques et participe au choix des produits de sécurité.
- Le CST est pilote du déploiement des produits de sécurité.

Profil du CST

- Spécialiste des techniques utilisées dans son aire de responsabilité.
- Sensibilisé aux bases de la sécurité des systèmes d'information.
- Motivé par les concepts liés à la sécurité des systèmes d'information.
- Curieux, communicatif et soucieux de s'investir dans la sécurisation des systèmes d'information.

Responsabilités du CST

- S'assurer que l'ensemble des nouveaux projets intègrent une composante sécurité.
- S'assurer que les opérations de maintenance et d'évolution des systèmes techniques se font en cohérence avec les exigences sécurité.
- Sensibiliser, conseiller et proposer des solutions aux problématiques de sécurité, directement ou en collaboration avec le RSSI.
- Aider les Chefs de Projets à intégrer la composante sécurité de l'initialisation aux phases finales des projets.
- Être en liaison avec les CSM ou CST impliqués lorsque cela est nécessaire.
- Se tenir au courant des évolutions du programme de sécurité.

Organisation

- Les CST sont nommés par le Management Informatique.
- Le CST prend connaissance des orientations du programme de sécurité et des standards propres à son aire de responsabilité.
- Le CST participe à la réunion mensuelle des CST et du Service Sécurité.
- CST UNIX, CST Novell, CST Réseau, CST NT, CST Technologies de Développement...

CSM

Correspondant

Sécurité

Métier



Rôle du CSM

- Promouvoir le programme de sécurité dans son aire de responsabilité.
- S'assurer de la mise en œuvre des orientations de sécurité.
- Collaborer activement avec le RSSI.

- Le CSM participe aux Comités de Suivi de l'ensemble des projets en cours dans son aire de responsabilité.
- Le CSM conseille le Service Sécurité sur les aspects métiers et applicatifs et participe aux éventuels choix de produits de sécurité.

Profil du CSM

- Spécialiste des processus et des applications utilisés dans son aire de responsabilité.
- Sensibilisé aux bases de la sécurité des systèmes d'information.
- Motivé par les concepts liés à la sécurité des systèmes d'information.
- Curieux, communicatif et soucieux de s'investir.

Responsabilités du CSM

- S'assurer que l'ensemble des nouveaux projets intègrent une composante sécurité.
- S'assurer que les opérations de maintenance et d'évolution des processus métier se font en cohérence avec les exigences sécurité.
- Sensibiliser, conseiller et proposer des solutions aux problématiques de sécurité, directement ou en collaboration avec le RSSI.
- Aider les Chefs de Projets à intégrer la composante sécurité de l'initialisation aux phases finales des projets.
- Être en liaison avec les CSM ou CST impliqués lorsque cela est nécessaire.
- Se tenir au courant des évolutions du programme de sécurité.

Organisation

- Le CSM est nommé par la Direction Générale.
- Le CSM prend connaissance des orientations du programme de sécurité et des standards propres à son aire de responsabilité.
- Le CSM participe à la réunion trimestrielle des CSM et du Service Sécurité.

CSE

Correspondant

Sécurité

Entité



Rôle du CSE

- Promouvoir le programme de sécurité du Groupe dans son entité.
- S'assurer de la mise en œuvre des orientations de sécurité.
- Collaborer activement avec le RSSI.

- Le CSE participe aux Comités de Suivi de l'ensemble des projets en cours dans sa filiale, au moins dans les phases initiales.
- Le CSE conseille le Service Sécurité sur les aspects locaux et participe aux éventuels choix de produits de sécurité adaptés à son environnement.

Profil du CSE

- Maîtrise globale des processus et des applications utilisés dans sa filiale.
- Sensibilisé aux bases de la sécurité des systèmes d'information.
- Motivé par les concepts liés à la sécurité des systèmes d'information.
- Curieux, communicatif et soucieux de s'investir.

Responsabilités du CSE

- S'assurer que l'ensemble des nouveaux projets intègrent une composante sécurité dans son entité.
- S'assurer que les opérations de maintenance et d'évolution des processus métier ou des architectures techniques locales se font en cohérence avec les exigences sécurité.
- Sensibiliser, conseiller et proposer des solutions aux problématiques sécurité, directement ou en collaboration avec le RSSI.
- Aider les Chefs de Projets à intégrer la composante sécurité de l'initialisation aux phases finales des projets.
- Être en liaison avec les CSM ou CST impliqués lorsque cela est nécessaire.
- Se tenir au courant des évolutions du programme de sécurité.

Organisation

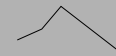
- Le CSE est nommé par la Direction Générale.
- Le CSE prend connaissance du Programme de Sécurité global.
- Le CSE participe à la conférence téléphonique mensuelle avec le Service Sécurité.
- Le CSE participe au meeting annuel organisé par le Service Sécurité.

Les Standards Applicables

Les projets fondateurs

« Ce sont les petites précautions qui
conservent les grandes vertus »

Jean-Jacques Rousseau



Les Standards Généraux

- Rédaction et classification des standards de sécurité de l'entreprise
- Standards « Politique Générale de Sécurité » - **STPGxx**
- Standards « Traitement et protection de l'information » - **STTPIxx**
- Standards « Sensibilisation » - **STSxx**
- Standards « Communication et reporting » - **STCRxx**
- Standards « Sécurité physique » - **STSPxx**
- Standards « Conformité aux lois et règles internes » - **STCxx**
- Standards « Infrastructure réseau et télécom » - **STRTxx**
- Standards « Applications et développements » - **STADxx**
- Standards « Continuité d'activité » - **STACxx**

Les Standards Techniques

- Rédaction et classification des standards techniques de l'entreprise
- Standards « UNIX » - **STUxx**
- Standards « NOVELL » - **STNxx**
- Standards « NT » - **STNTxx**
- Standards « Architecture Internet » - **STIxx**
- Standards « ... » - **ST...xx**

Qualification sécurité du réseau (LAN et WAN)

- Évaluation du niveau de sécurité du réseau de l'entreprise
- Étude du rapport d'évaluation et des préconisations
- Classification des préconisations
- Chiffrage des préconisations
- Priorisation des actions
- Planification des actions

Politique générale de sécurité : Actions

- Gestion du réseau des correspondants CSE, CSM, CST
- Définition et formation des propriétaires
- Définition et formation des gestionnaires
- Programme de sensibilisation
- Les Comités de Sécurité
- Veille technologique
- Sécurisation des infrastructures physiques
- Rédaction du Plan ou du Schéma Directeur et des budgets
- ...