Fonction
RSSI IV.A (H/F)

Évolutions possibles

Au sein du métier

- RSSI IV.A (H/F)
- RSSI IV.B (H/F)
- ADMINISTRATEUR SOLUTIONS DE SECURITE III.3 (H/F)
- ADMINISTRATEUR SOLUTIONS DE SECURITE IV.A (H/F)
- ANALYSTE DE LA MENACE III.3 (H/F)
- ANALYSTE DE LA MENACE IV.A (H/F)
- ANALYSTE REPONSE INCIDENT III.3 (H/F)
- ANALYSTE REPONSE INCIDENT IV.A (H/F)
- ANALYSTE SOC III.2 (H/F)
- ANALYSTE SOC III.3 (H/F)
- ANALYSTE SOC IV.A (H/F)
- CORRESPONDANT SECURITE III.2 (H/F)
- CORRESPONDANT SECURITE III.3 (H/F)
- CORRESPONDANT SECURITE IV.A (H/F)
- EXPERT CYBER IV.B (H/F)
- PENTESTEUR III.3 (H/F)
- PENTESTEUR IV.A (H/F)
- RESPONSABLE ANTICIPATION DETECTION ET REPONSE IV.A (H/F)
- RESPONSABLE ANTICIPATION DETECTION ET REPONSE IV.B (H/F)
- RESPONSABLE PROJET DE SECURITE III.3 (H/F)
- RESPONSABLE PROJET DE SECURITE IV.A (H/F)
- EXPERT CYBER IV.A (H/F)

Raisons d'être

Le RSSI définit les principes et règles de sécurité SI dans son domaine de responsabilité, et contrôle leur mise en œuvre.

Sensibilise et forme les acteurs concernés dans son domaine de responsabilité.

Entretient une veille pro-active en matière de sécurité SI, analyse les risques et propose des évolutions dans son domaine de responsabilité.

Le périmètre de responsabilité du RSSI peut s’exercer sur différents domaines en fonction de la nature de l’organisation.

Missions

Définit la politique de sécurité SI dans son domaine de responsabilité

- Décline les grandes orientations fixées au niveau de la Direction Générale de l’entreprise
- Participe à l’élaboration des règles de sécurité SI au niveau global du groupe
- Définit et met en place les principes et règles de sécurité SI applicables dans son domaine de responsabilité
- Participe à la réalisation de la charte de sécurité SI

Analyse les risques en matière de sécurité SI dans son domaine de responsabilité

- Analyse les risques dans son domaine de responsabilité
- Etablit des plans de réduction des risques

Contrôle l’application de la politique de sécurité SI dans son domaine de responsabilité

- Vérifie que les équipes appliquent les principes et règles de sécurité SI, la charte de sécurité SI et les plans de réduction des risques
- Effectue la validation des dispositifs de sécurité SI
- Planifie les audits sécurité
- Déclenche les cellules de crise en cas de sinistre sécurité SI

- Produit le reporting et les tableaux de bord de la sécurité SI

Organise les actions de sensibilisation et de formation à la sécurité SI

- Anime la filière SSI de son entité (correspondants SSI)
- Organise la formation à la sécurité SI dans son domaine de responsabilité
- Anime des réunions de sensibilisation / information à la sécurité SI
- Apporte assistance et conseil aux différents acteurs concernés

Assure une veille technologique et prospective en matière de sécurité SI

- Suit les évolutions réglementaires et techniques
- Propose les évolutions nécessaires pour garantir la sécurité SI dans son domaine de responsabilité

Compétences

Comportementales Socles

Orientation client
: Enrichir l'expérience client en adoptant une posture de service et de conseil et développer une relation de confiance durable. Anticiper, analyser, comprendre les besoins et attentes de ses clients pour apporter des réponses personnalisées. S'appliquer à améliorer la satisfaction client et mesurer son niveau de satisfaction.

Culture du changement et de l'innovation
: Encourager et accompagner le changement et les initiatives d'amélioration dans un environnement complexe et incertain. Expérimenter, tester, évaluer en s'appuyant sur de nouvelles méthodes, y compris numériques. Comprendre et susciter l'innovation en remettant en question les usages et en osant être pionnier. Etre dans une dynamique d'identification et d'apport de nouveautés dans son activité en osant sortir du cadre pour penser le problème en dehors de ses limites et de ses moyens lorsque la situation le demande.

Coopération et ouverture
: Construire et faire vivre des réseaux informels ou structurés d'individus ou de groupes en s'appuyant sur les outils collaboratifs comme les réseaux sociaux internes. Participer individuellement à l'atteinte d'un résultat collectif en favorisant l'entraide et le partage de connaissances. Savoir fédérer les parties prenantes d'un projet autour d'un objectif commun et établir des partenariats. Faire preuve d'écoute active vis-à-vis de ses interlocuteurs et prendre en compte leurs problématiques et les objections émises dans ses actions et prises de décision. Etre ouvert(e) d'esprit et curieux(se) au sein de son environnement.

Orientation résultats
: Engager des actions et mobiliser en toute autonomie des ressources (financières, matérielles, techniques, numériques et humaines) pour atteindre des performances durables dans le respect des principes éthiques, de qualité de vie et de RSE. Savoir être proactif et fixer, pour soi et/ou pour d'autres, des objectifs ambitieux et exploiter des opportunités pour aller au-delà des attendus.

Cyber Sécurité

Gestion de crise cyber
: Elaborer, mettre à l'essai et mettre en oeuvre les plans permettant à l'entreprise de se préparer et de faire face à la survenance d'une crise cyber (ex : roles et responsabilités, organisation d'exercices de crise, pilotage effectif de crise cyber, etc.)

Gestion des risques cyber et Système de Management de la Sécurité de l'Information (SMSI)
: Maitriser les principes, méthodes et outils d'évaluation et l'atténuation des risques (méthode Marion MEHARI, EBIOS...)., y compris l'évaluation des défaillances et de leurs conséquences. Mettre en place un système de management basé sur une approche du risque lié à l'activité, visant à établir, mettre en oeuvre, exploiter, surveiller, réexaminer, tenir à jour et améliorer la sécurité de l'information.

Compréhension des menaces cybersécurité
: Etre capable de d'identifier, analyser et anticiper les cybermenaces susceptibles de mettre en péril les intérêts de l'organisation et/ou des partenaires (ex : groupe d'attaquants, menace étatique, etc.)

Stratégie cybersécurité
: Définir une stratégie officielle permettant d'assurer la sécurité des systèmes et des données informatiques vis-à-vis de menaces extérieures ou intérieures et la rendre applicable via la déclinaison en plans d'actions.

Politiques de cybersécurité
: Créer, intégrer et appliquer des politiques qui répondent aux objectifs de sécurité de l'organisation. Maitriser le corpus documentaire cybersécurité existant.

Etat de l'art cybersécurité

Avoir une connaissance à 360 degrés, en permanence mise à jour, des principes fondateurs de la cybersécurité : risques cyber, menace, techniques d'attaque, organisation de la sécurité, normes en vigueur, corpus documentaire.

Efficacité professionnelle

Veille / innovation / tendances
: Se tenir informé(e) des tendances, des évolutions technologiques et des innovations en vigueur dans son domaine d'intervention en lien avec les enjeux de l'entreprise et attentes des clients / partenaires et à les intégrer dans son activité.

Transfert de compétences
: Maîtriser l'ensemble des techniques et outils et les leviers d'action permettant de faire preuve de pédagogie. Savoir transmettre des connaissances.

Analyse du besoin Client / Partenaire / Collaborateur
: Comprendre, analyser et challenger les besoins et attentes de ses clients / partenaires / collaborateurs, en prenant en considération leurs contraintes et les risques associés. Conseiller et alerter au regard de leurs choix.

Pilotage et gestion de l'activité

Relation partenaires / fournisseurs
: Sélectionner un partenaire/fournisseur en respectant la politique définie (sourcing, orientation make or buy, . . .). Piloter la relation (modes de fonctionnement, communication, gouvernance de pilotage. . .), anticiper les litiges, gérer les crises et alerter en cas de nécessité. Assurer le suivi contractuel de la relation avec les fournisseurs (contrats de projet, contrat de service, contrats fournisseurs internes, fournisseurs externes,. . .) et réaliser et analyser un bilan QCD (Qualité, Coûts, Délais).

Techniques SI

Organisation, principes et processus de traitement des incidents, des problèmes et des changements
: Concevoir et mettre en place l'organisation et les processus.

Contraintes légales et aspects juridiques liés à la sécurité
: Niveau de maitrise attendu : 3 Connaitre et appliquer la charte d'utilisation en matière de sécurité informatique, CNIL, archivage légal de documents, externalisation des données, respecter le RGPD, la réglementation autour des données...

Qualification du risque Métier associé à une solution
: Savoir qualifier le risque métier d'une solution à travers : - PCA (Plan de continuité d'activité). - PRA (Plan de reprise d'activité). - Réversibilité des contrats

Gestion des situations de tension organisationnelle ou humaine
: Gestion des situations de tension organisationnelle ou humaine

Environnement de travail

- Le RSSI est principalement en relation avec les Experts informatiques et les Spécialistes informatiques en matière de sécurité, les Responsables de domaine SI, les Chefs de projet SI, les Managers informatiques, les Architectes Fonctionnels SI et les Architectes informatiques
- Le RSSI peut être en relation avec toutes les autres fonctions de la filière SI, et de manière générale, avec toutes les fonctions de l’entreprise
- Le RSSI est en relation avec les organismes professionnels reconnus en matière de sécurité SI, les fournisseurs de solutions sécurité et d’autres RSSI externes

Famille

Filière

Métier

Répartition des effectifs

-

Bgpn reseau

-

Services-Courrier-Colis

-

Groupe - siege

Effectif de la fonction

De 1 à 9