IDENTIFICATION DU POSTE/GENERALITES		
Fonction	Responsable de la Sécurité des Systèmes d'Information	
Direction	Direction Générale	
Pôle / Département	Systèmes d'Information	
Poids du Poste	16	
Service		
Position dans l'organigramme	Hiérarchique N+1	Responsable de Sécurité des système d'information
	Sous sa responsabilité N-1	Collaborateurs directs : • Ingénieurs Sécurité

Missions du Poste
• Assurer la bonne gouvernance de la sécurité des systèmes d'information d'Orange RDC. • Contribuer à la définition de la stratégie d'évolution des systèmes d'informations d'Orange. • Contribuer à la définition des architectures des Services/applications du DRSI. • Contribuer à l'Audit et contrôle de conformité en Cybersécurité • Contribuer à la mise en œuvre et suivi du dispositif de sécurité Internet • Contribuer à la Construction des solutions de sécurité (choix techniques, architecturaux...) • Contribuer aux études techniques permettant au RSSI de faire les choix des dispositifs techniques les plus appropriés aux besoins de l'entreprise (firewall, cryptographie, authentification...). • Assurer la gestion des incidents de sécurité et leur correction dans le plus bref délais afin d'éviter tout impact négatif au sein de l'organisation • Faire évoluer les mesures et les normes de sécurité web et messagerie, en cohérence avec la nature de l'activité de l'entreprise et son exposition aux risques informatiques (politique de mots de passe, choix d'antivirus, certificats…). • Pilotage de la mise en place des éléments de sécurité (PKI, cartes à puces...) • Sécuriser les données personnelles, relatives à nos clients et aux salariés d'orange • Industrialiser et automatiser les Contrôles SOX DRSI. • Assurer la protection des actifs cœurs de réseaux et systèmes orange. • Définir l'architecture I@M locale, dans le respect de l'architecture cible I@M • S'assurer de la cohérence des différentes phases de ces développements • Etudier les adaptations du SI local nécessaires à la réalisation du projet I@M local • Coordonner les développements des composants locaux • S'assurer de la bonne interconnexion des moyens locaux avec les composants I@M centraux • Elaborer et gérer le budget et le planning permettant de réaliser l'ensemble du programme • Assurer le suivi de la mise en œuvre des recommandations et de la correction des vulnérabilités.

Activités du poste	
Activités de Delivery	• S'assurer que les risques du DRSI sont identifiés et gérés • Accompagner les missions d'audit, de sécurité et de conformité et assurer la mise en application des recommandations de ces audits • Participer à la coordination de la gestion des crises majeures. • Participer activement dans l'exécution des processus (conception, construction et mise en production) concernant le DRSI • Organiser et suivre les actions sécurité relatives au domaine du DRSI ; • Assurer la gestion des vulnérabilités ainsi que leurs fixations par les équipes en charge des plateformes concernées en heure et à temps • Analyser les risques et les dysfonctionnements, les marges d'amélioration des systèmes de sécurité

	• Accompagner les projets d'infrastructures sécuritaires • L'analyse et de la définition des rôles métiers ; • La définition des matrices de séparation des tâches ; • La conduite du changement induite par la mise en œuvre de la solution I@M, avec les actions de sensibilisation et de formation correspondantes. • Mettre en plan des solutions Cybersécurité par rapport aux exigences de sécurité du Groupe • Mettre en place les méthodes et outils de sécurité web adaptés et accompagner leur implémentation auprès des utilisateurs. • Participer à la définition et au contrôle de la gestion des habilitations • Rechercher des solutions innovantes pour répondre aux problématiques induites par l'introduction d'une nouvelle technologie • Revoir la gestion de l'intégrité des bases de données en renforçant la sécurité
Activités Run	• Elaborer et suivre des tableaux de bord des incidents sécurité • Superviser ou auditer les programmes de sauvegarde (back-up). • Faire analyser les causes des incidents et consolider les mesures de sécurité. • Faire tester régulièrement le bon fonctionnement des mesures de sécurité mises en place pour en détecter les faiblesses et les carences. • Auditer le respect des normes de sécurité informatique imposées aux sous-traitants de l'entreprise • Assurer une veille réglementaire sur la protection des données personnelles • Mettre en place un tableau de bord mensuel de pilotage des activités de sécurité • Participer et contribuer à la gestion des incidents et la gestion des problèmes DRSI • Participation à la construction des solutions de sécurité (choix techniques, architecturaux...) • Mettre en place un SIEM (Security Information and Event Management) pour la collecte, la corrélation des journaux des ressources informatiques • Faire des analyses en live des journaux par les SOC (Security Operations Center) • Mettre place d'une solution d'Authentification forte pour sécuriser les accès administrateurs et utilisations aux équipements et applications critiques • Analyse des processus locaux et garantir leur conformité au cadre des processus décrit dans la politique de gestion des identités et des accès (communément appelée Politique I@M). • Analyse et de la définition des rôles métiers • Définir des matrices de séparation des tâches • Conduire du changement induite par la mise en œuvre de la solution I@M, avec les actions de sensibilisation et de formation correspondantes
Gestion de la performance	• Contrôler les tableaux de bord techniques des incidents de sécurité rencontrés (virus, tentatives d'intrusion, …) • Mettre en place un tableau de bord journalier/hebdo/mensuel de pilotage des activités du service et définir les actions d'amélioration en fonctions des KPIs et des objectifs assignés au Service • Développer et suivre les indicateurs de performance clés en mettant l'accent sur la satisfaction de la demande des clients et la réalisation des activités • Elaborer et suivre des tableaux de bord des incidents sécurité

PRINCIPAUX CONTACTS	
Internes	• Toutes les Directions • Les équipes Réseaux • Les autres Départements et équipes IT

Externes	• Fournisseurs & partenaires • Groupe Orange et Skills Center • Filiales OMEA
COMPETENCES	
Profil	• Diplômé d'une école d'Ingénieur ou d'une école de commerce Bac +4/5 • Connaissance approfondie du SI, des plateformes de Service, plus largement de leur utilisation et impacts au sein de l'entreprise • Compétences managériales, développements des collaborateurs, coopération et influence en transverse, conduite du changement • Compétences en Project Delivery, en exploitation et Production SI • Connaissance des Méthodes & Outils Sécurité SI & Réseaux • Connaissance de l'élaboration et de la mise à jour des politiques et procédures ITIL • Expérience sur les réseaux GSM, GPRS, … • Connaissance des business models et de l'organisation globale des entreprises de télécommunication • Connaissance en terme de gestion des risques (Ebios ISO 27002) • Capacité d'analyse et de projection • Bonne culture SI, Réseau et Plateformes de service • Une certification en cyber sécurité sera un atout : CISSP, CEH, … • Parler couramment anglais
Savoirs Etre	• Charisme / leadership • Organisé et réfléchi • Forte implication dans son métier • Passionné par les nouvelles technologies • Adaptabilité / Esprit d'équipe / Réactivité / Créatif / Ambitieux • Rigueur/fiabilité / Intégritéé/ Capacité d'adaptation / Sens de l'organisation • Sens relationnel / Persuasif • Culture du résultat

AIRE DE MOBILITE	
Poste précédent	Chef de Projet SI/ Ingénieur/Support Développement
Evolution(s) possible(s)	Responsable de Sécurité des système d'information

Nom et prénom de l'agent	
Signature de l'agent	
Nom et prénom du supérieur hiérarchique	
Signature du supérieur hiérarchique	