

Fiche de poste

1. Identification du poste :

Titre du poste :	Ingénieur sécurité en système informatique
Direction	Direction générale
Superviseur immédiat	Coordonnateur Développement Système d'Information

2. Sommaire du profil du poste

Placé sous l'autorité hiérarchique du Coordonnateur Développement Système d'Information, l'ingénieur sécurité informatique a pour objectif de s'assurer que les procédures relatives à la sécurité informatique sont appliquées par toutes les parties prenantes et que la politique de gouvernance de la sécurité sont suivis et que de ces faits, le FID s'assure d'avoir un système répondant aux normes requises. Il se charge pour cela de piloter la mise en place de la politique générale de la sécurité et le suivi de ses applications, de mettre en œuvre la mise en normes et standards du système informatique aux niveaux de la Direction Générale, des DIRs et acteurs du FID en général et d'assurer la sécurisation de tous les serveurs et les postes de travail du FID.

3. Description spécifique des activités principales

Conception et mise à jour de la politique de sécurisation informatique

- Charger d'étudier la mise en œuvre et la sécurisation de différents systèmes selon les normes et standards de sécurités
- Identifier les risques et définir de la Politique de sécurité ;
- Mettre en œuvre et Suivre le dispositif de sécurité ;
- Prendre en charge une liste de projets déjà identifiés afin de permettre au FID de poursuivre l'amélioration et la modernisation de ses systèmes d'information.
- Analyser les risques et les dysfonctionnements, les marges d'amélioration des systèmes de sécurité ;
- Définir et faire évoluer la Politique de Sécurité des Systèmes d'Information du FID (PSSI) ;
- Effectuer des évaluations des risques de sécurité informatique et proposer les moyens de prévention et de réduire les menaces ;
- Concevoir et veiller à la mise à jour permanente des outils de suivis de la sécurité informatique
- Assurer la rédaction, la mise à jour et l'application des manuels de procédure de la sécurité informatique

Contrôle de l'effectivité des mesures de sécurisations informatiques par l'ensemble du programme

- Établir un Plan de prévention des risques informatique et un Plan de continuité d'activité (PCA) ou Plan de maintien en conditions opérationnelles du SI (PCA/RAS) ;
- S'assurer la mise en place de la Politique et des Procédures de sécurité ;
- Participer aux actions d'administration système lié aux audits et la mise en œuvre des évolutions techniques, test, essai et amélioration
- Participer à la validation des applications déployées sur les postes de travail et sur les serveurs
- Assurer la sécurisation des serveurs et des postes de travail
- Analyser les risques, les dysfonctionnements, les failles dans la protection, les marges d'amélioration des systèmes de sécurité pour garantir enfin la confidentialité et l'intégrité des données
- Réaliser des supports de formation et en assurer la diffusion principalement auprès des collègues du service informatique
- Suivre la conformité de la Charte de sécurité infra et Système d'Informations : "Access right", Username, Password, par rapport aux TDR des utilisateurs.

Participer à la conception et maintenance du réseau informatique

- Participer à l'élaboration et/ou à la validation des cahiers de charges des matériels et logiciels à acquérir
- Participer à la formation des utilisateurs du SI sur la thématique intéressant la sécurité informatique la cybercriminalité
- Assurer la résolution des problèmes liés à la sécurité informatique
- Surveiller les vulnérabilités de Sécurité et piratage sur les infrastructures : faire tester régulièrement le bon fonctionnement des mesures de sécurité mises en place pour en détecter les faiblesses et les carences (tests d'intrusion notamment = IDS).

- Identifier les nouveaux risques sur la sécurité du système d'information : apparition de nouveaux virus, lancement d'attaques informatiques sur le réseau WAN
- Suivre et relever les différents incidents informatiques suivant le tableau de bord informatique et rapporter ces incidents

4. Profil de l'emploi :

Qualifications et expériences minimales requises :

Éducation et niveau de formation :	Ingénieur informaticien (BAC+5) titulaire de diplôme délivré par un établissement agréé
------------------------------------	---

Spécialités recherchées:	<ul style="list-style-type: none"> • Cinq années en sécurité informatique • Compétence en trois ans en administration de réseaux informatiques • Connaissance en cryptographie/cryptanalyse (chiffrement symétrique et asymétrique) • Connaissance de SQL et database administration • Connaissance des protocoles et systèmes de réseaux • Connaissance des applications web • Filtrage de contenu web • Connaissance système de virtualisation • Trois ans en administration de serveur sous Linux • Très bonne connaissance des équipements et outils de sécurité : Firewall, WAF, IDS/IPS, 2FA, Proxy, SIEM, IDS etc.
Expérience dans les spécialités recherchées:	5 ans et plus

Connaissances acquises ou à acquérir

- | | |
|--|--|
| <ul style="list-style-type: none"> • PAD • Rapports d'évaluation et/ou d'audit internes et externes • Manuels de procédures du FID. • Connaissance de l'organisation (mission, structure). | <ul style="list-style-type: none"> • Techniques de résolution de problèmes. • Techniques de communication. • Processus budgétaire. • Processus d'élaboration du PTA • Exigences en matière de rapports. |
|--|--|

Habilités

Analyse / synthèse
Créativité
Esprit de contrôle
Esprit d'équipe
Jugement/discernement

Attitudes/valeurs

Courtoisie/Diplomatie
Ponctualité dans le travail
Rigueur
Discrétion/confidentialité
Efficacité/Efficiency

Profil :

- Très bon compétence en Infrastructures Système et réseau informatique ;
- Excellente maîtrise de base Windows, Linux, Cloud Computing et Virtualisation ;
- Très bonne connaissances au norme de la sécurité des systèmes d'information (COBIT 5, ISO/IEC 27001 Series) ; une certification ITIL ou CISA ou CISM ou Autre serait un plus ;
- Bonne connaissance à l'Administration des infrastructures Telcom/Système/Virtualisation

Fiche d'Évaluation

1. Identification du poste :

Titre du poste : Ingénieur sécurité en système informatique
 Direction : Direction générale
 Superviseur immédiat : Coordonnateur Développement Système d'Information

Section A : Critères liés à l'accomplissement de la fiche de poste

1 = Faible 2 = A améliorer 3 = Satisfaisant 4 = Supérieur 5 = Exceptionnel

1. Sécuriser le système informatique	1	2	3	4	5
2. Concevoir et veiller à la mise à jour permanente des outils de suivi de la sécurité	1	2	3	4	5
3. Participer à l'élaboration et/ou à la validation des cahiers de charges des matériels et logiciels à acquérir	1	2	3	4	5
4. Assurer la rédaction, la mise à jour et l'application des manuels de procédure de la sécurité informatique	1	2	3	4	5
5. Assurer la résolution des problèmes liés à la sécurité informatique.	1	2	3	4	5
6. Capacité d'analyser les risques, les dysfonctionnements et les marges d'améliorations dans le SI	1	2	3	4	5

Total (de 5 à 30 points)

Section B : Critères liés au comportement et aux attitudes du Consultant

1 = Faible 2 = A améliorer 3 = Satisfaisant 4 = Supérieur 5 = Exceptionnel

1. Sens des responsabilités et sens aigu de la communication	1	2	3	4	5
2. Leadership/capacité à mobiliser/supervision du personnel	1	2	3	4	5
3. Esprit d'initiative, d'innovation ou autonomie dans son travail	1	2	3	4	5
4. Esprit de planification et de contrôle	1	2	3	4	5
5. Esprit d'équipe	1	2	3	4	5

Total (de 5 à 25 points)

C-1 : Le niveau du rendement du Consultant est la somme des évaluations des Sections «A», «B»

La note du consultant à la «Section A» est de :		sur 30 points
La note du consultant à la «Section B» est de :		sur 25 points
Total des critères d'évaluation du Consultant		Sur 55 points
L'appréciation générale du Consultant est la somme de :		sur 55 points

Section C-2 : Classification finale

Une note en bas de	20	est égale à la notation de :	1 =	Faible
Une note de	21	à 29	est égale à la notation de :	2 = À améliorer
Une note de	30	à 38	est égale à la notation de :	3 = Satisfaisant

Une note de	39	à	47	est égale à la notation de :	4 =	Supérieur
Une note de plus de :	48			est égale à la notation de :	5 =	Exceptionnel

Section D-1 : Commentaires du consultant(e) sur l'entrevue

--

J'ai lu cette fiche d'évaluation et en ai discuté avec mon chef hiérarchique

Signature du consultant :

Date :

Section D-2 : Commentaires généraux du Directeur et superviseur hiérarchique

Points forts du consultant	
Points à améliorer	
Évaluation générale	
Actions à mener pour améliorer la performance	

Signature du superviseur hiérarchique :

Date :

D-3: Validation/approbation du Directeur et du DG

Signature du Directeur :

Date :

Signature du DG :

Date :