Chef Département Sécurité Réseaux et SI

FICHE DE POSTE	
Supérieur hiérarchique	Directeur des Réseaux et du Système d'Information
Relation fonctionnelle	Toutes les structures SBIN, Fournisseurs, Gestionnaire, etc.

MISSIONS DU POSTE

- La mission première est de définir la politique de sécurité des Réseaux et du SI, et de veiller à son application.
- Le RSSI assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte. Il peut intervenir directement sur tout ou partie des systèmes informatiques et télécoms de son entité
- Il doit mener des actions de sensibilisation des différents acteurs de l'entreprise à la sécurité des réseaux et des systèmes d'information
- Il doit protéger les données sensibles de l'entreprise et gouverner leurs accès et utilisations
- Il doit garantir la sécurité physique et logique des infrastructures techniques et logicielle de l'entreprise
- Il doit mener des activités de veille technologique et opérationnelle pour mieux asseoir sa politique
- Et mettre en place une organisation permettant d'assurer, dans la durée, la gouvernance de la sécurité ITN

PRINCIPALES ACTIVITES

- Définir la politique de sécurité
  - Définir les objectifs et les besoins liés à la sécurité de l'entreprise
  - Définir et mettre en place les procédures liées à la sécurité des Réseaux et SI
  - Contribuer à l'organisation et à la politique de sécurité de l'entreprise
- Analyser de risques
  - Evaluer les risques, les menaces et leurs conséquences
  - Etudier les moyens assurant la sécurité
  - Mettre en place des plans de mitigation pour les maitriser
- Sensibiliser et former aux enjeux de la sécurité
  - Informer et sensibiliser la direction générale sur les risques et menaces
  - Former les directions opérationnelles et métiers sur la Sécurité
  - Participer à la réalisation de la charte de sécurité de l'entreprise
  - Assurer la promotion de la charte de sécurité informatique auprès de tous les utilisateurs
- Etudier des moyens et faire de préconisations
  - Valider techniquement les outils de sécurité
  - Définir les normes et les standards de sécurité
  - Définir les exigences de sécurité et s'assurer de leur prise en charge dans les projets
- Auditer et contrôler

- Contrôler et garantir que les équipes appliquent les principes et règles de sécurité
- Auditer la vulnérabilité de l'entreprise
- Réaliser des audits réguliers pour évoluer les risques, les menaces et les vulnérabilités
- Déclencher les cellules/comité de crise en cas de sinistre sécurité Réseaux et SI

- Faire de la veille technologique et prospective
  - Effectuer le suivi des évolutions réglementaires et techniques de son domaine
  - Veiller sur les évolutions nécessaires pour garantir la sécurité logique et physique des Réseaux et SI dans leur ensemble
- Accompagner à la transformation
  - Diffuser la culture sécurité auprès des différents acteurs de l'entreprise
  - Accompagner la digitalisation de l'entreprise tout en s'assurant que les problématiques de sécurité, de cybersécurité sont bien pris en charge
  - Organiser la montée en compétence des équipes techniques et fonctionnelles
- Gérer de la performance
  - Tenir et communiquer un TDB sur les intrusions constatées sur une période donnée
  - Mesurer de façon continue le niveau d'appropriation de la politique de sécurité informatique par les utilisateurs
  - Suivre les performances des politiques mises en place et leur effectivité
  - Piloter la mise en place, le suivi de la réalisation de son budget (OPEX et CAPEX)

PROFIL DU TITULAIRE DU POSTE	
Formation	• Ingénieur ou équivalent Bac+5 en informatique ou Diplômé d'une école d'Ingénieur ou d'une école de commerce Bac +5
Expériences professionnelles	• Justifier d'un minimum de 7 années d'expérience professionnelle dans le domaine de la sécurité ou cybersécurité ;
Compétences requises	• Veille technologique - Analyser les développements technologiques informatiques les plus récents afin de pouvoir comprendre les technologies innovantes. Rechercher des solutions innovatrices pour l'intégration d'une nouvelle technologie dans les produits, applications ou services existants ou pour la création de nouvelles solutions. • Développement de la stratégie pour la sécurité de l'information - Définir et fait appliquer une stratégie officielle permettant de maintenir la sécurité et l'intégrité de l'information, en en précisant sa portée et en instaurant une culture. - Définir les règles du système de gestion de la sécurité de l'information, y compris l'identification des rôles et les responsabilités. Utiliser des normes pour fixer des objectifs d'intégrité, de disponibilité et de confidentialité des données propres à l'entreprise.

	• Développement du personnel - Etablir un diagnostic des compétences individuelles et collectives, par identification des besoins et lacunes. - Etudier les possibilités de formation et de perfectionnement et sélectionne la méthodologie appropriée, en tenant compte des besoins de l'individu et de l'entreprise. - Conseiller et/ou guider les individus et les équipes pour répondre aux besoins en matière de formation. • Gestion des Risques - Mettre en œuvre la gestion des risques dans les systèmes d'information en appliquant la politique et les procédures de gestion des risques définies par l'entreprise. - Evaluer les risques pour l'activité de l'organisation, documenter les risques possibles et les plans d'actions pour les contrôler • Gestion de la sécurité de l'information - Mettre en œuvre la politique de sécurité de l'information. - Contrôler et prendre des mesures contre les intrusions, les fraudes, les atteintes ou les fuites concernant la sécurité. - Garantir l'analyse et la gestion des risques concernant la sécurité des données et des informations de l'entreprise. - Mettre en œuvre la politique de sécurité de l'information. - Contrôler et prendre des mesures contre les intrusions, les fraudes, les atteintes ou les fuites concernant la sécurité. - Garantir l'analyse et la gestion des risques concernant la sécurité des données et des informations de l'entreprise. - Passer en revue les incidents de sécurité et formuler des recommandations pour une amélioration continue de la sécurité. • Gouvernance - Définir, mettre en place et contrôler la gestion des réseaux et systèmes d'information en ligne avec les ambitions de l'entreprise. - Tenir compte de tous les paramètres internes et externes tels que la conformité aux normes légales et industrielles afin d'orienter la gestion des risques et le déploiement de ressources de façon à apporter le bon niveau de service à l'entreprise • Savoirs être - Charisme / leadership - Organisé et réfléchi - Forte implication dans son métier - Passionné par les nouvelles technologies - Adaptabilité / Esprit d'équipe / Réactivité / Créatif / Ambitieux

	- Rigueur/fiabilité / Capacité d'adaptation / Sens de l'organisation - Sens relationnel / Persuasif - Culture du résultat
LIEU DU CONTRAT	
Lieu	Cotonou
Disponibilité du candidat	Immédiate ou selon la durée du préavis
Dossier à fournir	• Un CV actualisé • Une lettre de motivation Si vous vous reconnaissez dans cette offre, rejoignez-nous en envoyant votre dossier de candidature à l'adresse : recrutetalents@sbin.bj avec pour objet du mail, la mention : "**Candidature au poste de Chef Département Sécurité Réseaux et SI** " au plus tard le **09 novembre 2021 à 20h00** (heure de Cotonou).