|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **DESCRIPCION DE PUESTO**  **ESPECIALISTA DE CIBERSEGURIDAD EMPRESA WHITEHAT SECURITY** | | | | | | | | | | | | | | | |
| **INFORMACION GENERAL** | | | | | | | | | | | | | | | |
| **Título de Cargo:** | | Especialista en Ciberseguridad | | | | | | |  | | |  | | | |
| **Área:** | | Seguridad de la información | | | | | | | | | | | | | |
| **Departamento:** | | Tecnologías de la información | | | | | | | | | | | | | |
| **Código de Cargo:** | | CYB0001 | | | | | | |  | | | |  | | |
| **Centro de Costo** |  | GUA00001 | | | | | | |  | | | |  | | |
| C**AMPO DE ACCIÓN** | | | | | | | | | | | | | | | |
|  | | | | | | | | | | | | | | | |
| * **Número de Subordinados :**    + Directos: 1   + Indirectos: 1   + Terceros: * **Salario:**    + $4953 - $9245 * **Ayuda de Costo:**   + Dejar en blanco * **Grade del cargo:**   + Dejar en blanco * **Aplica gestión metas:**   + SI ( X ) NO ( ) * **Gestión en Países:**    + Centro América   + Otro * **Debe viajar**   + SI ( ) NO ( X ) | | | | | | * **Debe viajar**   + Local ( )   + Internacional ( ) * **Jefe Inmediato:**   + Jefe de Ciberseguridad * **Presupuesto anual a su cargo :**   + Directo   + Indirecto   + US$ 56,900,000 * **% Bono**   + 20% * **Acceso a SAP**   + SI ( ) NO ( X )   + Especificar modulo: | | | | | | | | | |
| **INDICADORES CLAVE DEL NEGOCIO:** | | | | | | | | | | | | | | | |
| * Presupuesto: US$50,000,000 * Numero de incidentes de seguridad resueltos. * Numero de incidentes de seguridad prevenidos. * Tiempo promedio de respuesta a incidentes. | | | | | | | | | | | | | | | |
| **RED DE CONTACTOS INTERNOS** | | | | | | | | | | | | | | | |
| * Áreas de TI, Operaciones, Desarrollo de Software, Compliance, Legal | | | | | | | | | | | | | | | |
| **RED DE CONTACTOS EXTERNOS** | | | | | | | | | | | | | | | |
| * Proveedores de seguridad, consultores de ciberseguridad, organizaciones de estándares de seguridad | | | | | | | | | | | | | | | |
| **PROPOSITO DEL PUESTO:** | | | | | | | | | | | | | | | |
| * Asegurar la protección de la infraestructura de TI y los datos corporativos frente a ciberataques. * Gestionar la respuesta a incidentes de seguridad y la recuperación ante desastres. * Implementar políticas y procedimientos de ciberseguridad. | | | | | | | | | | | | | | | |
| **PRINCIPALES DESAFÍOS DEL PUESTO:** | | | | | | | | | | | | | | | |
| * Ser el soporte de la toma de decisiones basado en el análisis completo de la seguridad de la información, amenazas cibernéticas y cumplimiento de las políticas de ciberseguridad de la empresa. | | | | | | | | | | | | | | | |
| **METAS HAZ (Colocar solo descripción general de la meta, no memorias de cálculo ni valores)** | | | | | | | | | | | | | | | |
| * META 1: Reducción de incidentes de seguridad por trimestre. * META 2: Aumento del nivel de cumplimiento de las políticas de seguridad * META 3: Mejora en los tiempos de respuesta a incidentes. * META 4: Implementación de nuevas tecnologías de protección de la información. * Meta 5: Cumplir con todos los estándares de seguridad y regulaciones pertinentes. | | | | | | | | | | | | | | | |
| **RESPONSABILIDADES ANUALES** | | | | | | | | | | | | | | | |
| * Desarrollo y revisión de la estrategia de ciberseguridad de la empresa. * Análisis del presupuesto anual en ciberseguridad. * Auditorias de seguridad y evaluación de riesgo. | | | | | | | | | | | | | | | |
| **RESPONSABILIDAD TRIMESTRAL** | | | | | | | | | | | | | | | |
| * Ajuste de las estrategias de protección en función de las tendencias emergentes en ciberseguridad. * Revisión trimestral de la efectividad de las políticas de seguridad. | | | | | | | | | | | | | | | |
| **RESPONSABILIDAD MENSUAL** | | | | | | | | | | | | | | | |
| * Revisión mensual de los controles de acceso y las políticas de seguridad. * Actualización de las medidas de seguridad basadas en las nuevas amenazas y vulnerabilidades. * Revisión de los informes de incidentes de seguridad y acciones correctivas. * Evaluación de la seguridad de la infraestructura TI mensualmente. | | | | | | | | | | | | | | | |
| **RESPONSABILIDAD QUINCENAL** | | | | | | | | | | | | | | | |
| * Revisar y actualizar la configuración de seguridad de los sistemas críticos. * Entrenamiento y concienciación de los empleados sobre ciberseguridad. | | | | | | | | | | | | | | | |
| **RESPONSABILIDAD DIARIA** | | | | | | | | | | | | | | | |
| * Monitoreo continuo de la red y sistemas para detectar actividades sospechosas. * Gestión de incidentes de seguridad de información. | | | | | | | | | | | | | | | |
| **COMPETENCIAS (lee descripción de competencias al final del documento, este campo es obligatorio)** | | | **Escala de Competencias requeridas para el puesto** | | | | | | | | | | | | |
| **1** | **2** | | | **3** | | | | **4** | | | | **5** |
| 1. Análisis y resolución de problemas | | | ( ) | ( ) | | | ( ) | | | | ( X ) | | | | ( ) |
| 1. Innovación tecnológica | | | ( ) | ( ) | | | ( ) | | | | ( X ) | | | | ( ) |
| 1. Comunicación Efectiva | | | ( ) | ( ) | | | ( ) | | | | ( X ) | | | | ( ) |
| 1. Orientación Estratégica | | | ( ) | ( ) | | | ( ) | | | | ( ) | | | | ( X ) |
| 1. Gestión de Riesgos | | | ( ) | ( ) | | | ( ) | | | | ( ) | | | | ( X ) |
| 1. Trabajo en equipo y colaboración | | | ( ) | ( ) | | | ( ) | | | | ( ) | | | | ( X ) |
| **CONOCIMIENTO Y HABILIDADES** | | | **Escala de Conocimientos Requeridos para el puesto** | | | | | | | | | | | | |
| **1** | | **2** | | | **3** | | **4** | | | | **5** | |
| 1. Ciberseguridad y Protección de Datos | | | ( ) | | ( ) | | | ( ) | | ( ) | | | | ( X ) | |
| 1. Análisis de riesgos y vulnerabilidades | | | ( ) | | ( ) | | | ( ) | | ( ) | | | | ( X ) | |
| 1. Gestión de incidentes de seguridad | | | ( ) | | ( ) | | | ( ) | | ( ) | | | | ( X ) | |
| 1. Conocimiento de Normativas de seguridad. | | | ( ) | | ( ) | | | ( ) | | ( ) | | | | ( X ) | |
| 1. Auditorias de Seguridad informática. | | | ( ) | | ( ) | | | ( ) | | ( X ) | | | | ( ) | |
| 1. Manejo de Herramientas de seguridad | | | ( ) | | ( ) | | | ( ) | | ( ) | | | | ( X ) | |
| 1. Redes y Comunicaciones | | | ( ) | | ( ) | | | ( ) | | ( X ) | | | | ( ) | |
| 1. Criptografía y Control de accesos | | | ( ) | | ( ) | | | ( ) | | ( X ) | | | | ( ) | |
| **FORMACIÓN ACADEMICA** | | | | | | | | | | | | | | | |
| ( ) Primaria  ( ) Secundaria  ( X ) Título a nivel medio  ( X ) Pensum Cerrado ( X ) Graduado ( ) MBA  Cite especialización: Ciberseguridad / Sistemas de información / ingeniería informática | | | | | | | | | | | | | | | |
| **OTROS CONOCIMIENTO S REQUERIDOS** | | | | | | | | | | | | | | | |
| Anotar cualquier otro conocimiento requerido para la posición.  ( X ) Idiomas  Ingles  ( X ) Computación  Cite Programa y nivel de dominio: Herramientas de seguridad cibernética, conocimiento avanzado en sistemas de detección de intrusos, análisis de malware, uso de sistemas de prevención de intrusiones. | | | | | | | | | | | | | | | |
| **EXPERIENCIA LABORAL** | | | | | | | | | | | | | | | |
| Analista de ciberseguridad, ingeniero de seguridad de TI, Consultor de Ciberseguridad | | | | | | | | | | | | | | | |

|  |
| --- |
| **ORGANIGRAMA (Por favor incluir ubicación del puesto en el organigrama del área)** |
|  |

|  |  |  |  |
| --- | --- | --- | --- |
| **AUTORIZACIÓN** | | | |
| **Cargo& Área:**  Vicepresidente Manufactura | **Nombre:**  xxx | **Firma:** | **Fecha:** |
| **Cargo & Área:**  Gerente Planta Mariposa | **Nombre:**  xxx | **Firma:** | **Fecha:** |
| **Cargo & Área:**  Puesto X | **Nombre:**  xxx | **Firma:** | **Fecha:**  05/02/2024 |

|  |
| --- |
| **DEFINICIÓN DE COMPETENCIAS CABCORP** |
| **ANÁLISIS Y RESOLUCIÓN DE PROBLEMAS:**  Capacidad para identificar problemas de seguridad complejos y desarrollar soluciones efectivas. |
| **INNOVACIÓN TECNOLÓGICA:**  Está al día con las últimas tendencias en ciberseguridad y tecnologías emergentes. |
| **COMUNICACIÓN EFECTIVA:**  Comunica de manera clara y efectiva las políticas y procedimientos de seguridad a todos los niveles de la organización. |
| **ORIENTACIÓN ESTRATÉGICA:**  Entiende y alinea las iniciativas de ciberseguridad con los objetivos y estrategias del negocio. |
| **GESTIÓN DE RIESGOS:**  Evalúa y maneja de manera proactiva los riesgos de seguridad informática para la organización. |
| **TRABAJO EN EQUIPO Y COLABORACIÓN:**  Colabora eficazmente con equipos interdisciplinarios para mejorar la seguridad. |

|  |
| --- |
| **DEFINICIÓN DE PUNTUACIÓN** |
| **1:** Dominio no indispensable de la competencia.  **2:** Se requiere un dominio a nivel básico de la competencia.  **3:** Se requiere un dominio a nivel intermedio de la competencia y la practica regularmente.  **4:** Se requiere un domino a nivel avanzado de la competencia y siempre debe estar presente en su conducta.  **5:** Se requiere un domino a nivel avanzado de la competencia y desarrolla a otros en la misma. |