Responsabilidades y Calificaciones del CISO según Heller Search

1

RESPONSABILIDADES CLAVE I

- Desarrollar e implementar una estrategia y una hoja de ruta estratégicas de seguridad de la información a mediano y largo plazo para garantizar que los activos de información de la organización estén adecuadamente protegidos.
- Trabajar con líderes senior del negocio para evaluar y comunicar niveles aceptables de riesgo.
- Identificar, evalúa e informar sobre riesgos, prácticas y proyectos de seguridad de la información al Comité Ejecutivo y la Junta Directiva, y proporcionar experiencia en la materia sobre estándares de seguridad y mejores prácticas.
- Desarrollar, orientar y gestionar un personal de alto rendimiento de profesionales de seguridad de la información.
- Presidir el comité directivo de seguridad de la información (o junta de gobierno, o junta asesora).
- Desarrollar la comprensión de la Junta sobre la seguridad más allá de una visión de “solo cumplimiento”.
- Liderar el desarrollo de políticas, procedimientos, estándares y directrices de seguridad de la información actualizados, y supervisar su aprobación, difusión y mantenimiento.
- Asegurar que el programa de gestión de seguridad cumple con las leyes, regulaciones y requisitos contractuales aplicables.
- Actuar como líder del programa de seguridad de la información empresarial y fomentar una cultura consciente de la seguridad.
- Supervisar la evaluación, selección e implementación de soluciones de seguridad de la información que sean innovadoras, rentables y mínimamente disruptivas.

2

RESPONSABILIDADES CLAVE II

- Asociarse con arquitectos empresariales, infraestructura y equipos de aplicaciones para garantizar que las tecnologías se desarrollen y mantengan de acuerdo con políticas y directrices de seguridad.
- Administrar informes periódicos de detección de intrusiones y vulnerabilidades, revisiones de grupos de auditoría de TI internas y externas y la coordinación de todas las correcciones necesarias.
- Desarrollar métricas de negocio para medir la eficacia del programa de gestión de seguridad y aumentar la madurez del programa con el tiempo.
- Supervisar la industria y el entorno externo para detectar amenazas emergentes y asesorar a las partes interesadas relevantes sobre cursos de acción apropiados.
- Servir de enlace con aplicación de la ley y otros órganos asesores según sea necesario para garantizar que la organización mantiene una postura de seguridad fuerte.
- Supervisar la planificación de respuesta a incidentes y la investigación de violaciones de seguridad, y ayudar con cualquier disciplina disciplinaria, relaciones públicas y asuntos legales.
- Supervisar y liderar la creación, comunicación e implementación de un proceso para gestionar el riesgo del proveedor y otros riesgos de terceros.
- Liderar la debida diligencia y las actividades posteriores a la integración relacionadas con la seguridad de la información para todas las actividades de fusiones y adquisiciones.

3

CALIFICACIONES I

- Licenciatura en informática, ingeniería o un campo relacionado; (preferiblemente título de posgrado).
- Mínimo 10 años de experiencia en TI y/o liderazgo empresarial, y más de 5 años de experiencia en seguridad de la información/ciberseguridad.
- Un historial probado en el desarrollo de políticas y procedimientos de seguridad de la información y ejecución exitosa.
- Amplio conocimiento del riesgo empresarial, evaluación de riesgos y toma de decisiones basada en riesgos.
- Capaz de comunicar conceptos relacionados con riesgos y seguridad a audiencias tanto técnicas como no técnicas (en términos comerciales), incluido el nivel de junta directiva.
- Un influencer natural y constructor de coaliciones; Apasionado por construir equipos de alto rendimiento.
- Capacidad para inspirar y motivar equipos multifuncionales e interdisciplinarios para lograr objetivos tácticos y estratégicos; un líder innovador, solucionador de problemas y consultor.

4

CALIFICACIONES II

- Capacidad para evangelizar la seguridad de TI para convertirla en una parte crítica de las operaciones comerciales; generar confianza y respeto por la función de seguridad.
- Excelente comunicación escrita y verbal, habilidades interpersonales y colaborativas.
- Experimentado en negociaciones de contratos y proveedores.
- Capacidad para priorizar y ejecutar tareas de manera efectiva en situaciones de alta presión.
- Conocimiento de marcos y estándares de seguridad, riesgos y control como ISO 27001 y 27002, CIS, NIST, COBIT, COSO e ITIL.
- Comprensión de las arquitecturas de nube, SaaS e IoT y sus implicaciones en la estrategia de seguridad de la información.
- Perspicacia técnica que incluye, entre otros: OSI, infraestructura de TI, nube, lenguajes, herramientas y marcos de desarrollo de aplicaciones, tecnologías de bases de datos, tecnologías web, dispositivos móviles de próxima generación, arquitectura de red, arquitectura empresarial y servicios de directorio.
- Perspicacia y experiencia en tecnología de seguridad que incluyen, entre otros: firewall, detección de intrusiones, herramientas y defensas contra ataques cibernéticos, cifrado, autoridad de certificación, filtrado web, antimalware, antiphishing, gestión de identidad y acceso, autenticación multifactor.