EXPERTO (A) EN SEGURIDAD DE LA INFORMACIÓN (CISO)

NIVEL OCUPACIONAL
Superior Ejecutivo

CATEGORÍA
37 o 41 / 437 o 441

ROL
Experto(a) en Seguridad de la Información.

NATURALEZA
DE LA CLASE

Responsable de alinear la seguridad de la información con los objetivos del negocio, mediante la planeación, coordinación y administración de los procesos a su cargo, garantizando en todo momento que la información de la compañía esté adecuadamente protegida ante amenazas, y difundir la cultura de seguridad de la información a todos los miembros de la organización.

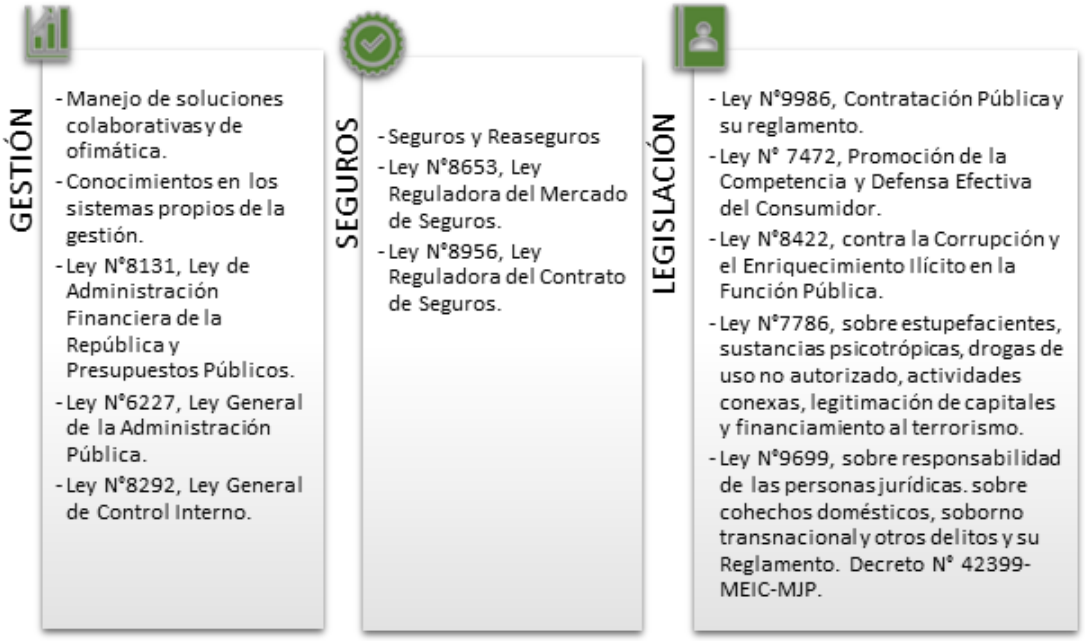
REQUISITOS
OBLIGATORIOS

- Licenciatura o grado superior en Ciencias de la Computación o carrera universitaria afín que lo faculte para el desempeño del puesto.
- Incorporado al colegio profesional respectivo en el grado correspondiente y al día con sus obligaciones de colegiatura.
- Certificado ISO 27001 LI ó ISO 27001 AI.
- Certificado CSX.
- Contar con algunas de las siguientes certificaciones: CDEPSE, CISM o CISSP.
- Mínimo 60 meses de experiencia en temas de seguridad de TI y de la Información, específicamente en las áreas de:
    - Gestión de proyectos de Seguridad de la Información.
    - Análisis y tratamiento de riesgos de Seguridad de la Información.
    - Evaluación de controles de Seguridad de la Información.
    - Alineación entre negocio y seguridad de la Información.
    - Seguimiento e implementación de acciones correctivas relacionadas con la Seguridad de la Información.
    - Diseño e implementación de sistemas de gestión de seguridad de la información.
    - Aseguramiento de la seguridad de la información.
- Mínimo 30 meses de experiencia en puestos de liderazgo.

REQUISITOS
DESEABLES

- Conocimiento en COBIT.
- Certificado en gestión de riesgos ISO 31000 ó CRISC.
- Conocimiento en redacción de informes técnicos.
- Conocimiento de la Ley N° 8968, Ley de Protección de la Persona Frente al Tratamiento de sus Datos Personales.
- Licencia de conducir B1 al día.

CONOCIMIENTOS
GENERALES



COMPETENCIAS

Este puesto exige un nivel 2 de desarrollo en:

RESPONSABILIDADES

ESPECÍFICAS

- Generar e implementar políticas y estándares de seguridad de la información, a fin de garantizar la seguridad y privacidad de la información y los datos.

- Desarrollar y liderar una visión y estrategia de seguridad de la información que esté alineada con los objetivos de la organización y facilite el alcance de las metas.

- Desarrollar, implementar y supervisar un programa estratégico y completo de seguridad de la información para garantizar niveles adecuados de confidencialidad, integridad, disponibilidad, seguridad, privacidad y recuperación de activos de información; propiedad, controlados y/o procesados por la organización.

- Determinar el enfoque de seguridad de la información y el modelo operativo en consulta con las partes interesadas y alineado con el enfoque de gestión de riesgos y la supervisión del cumplimiento de las áreas de riesgo non-digital.

- Definir, mantener y supervisar la arquitectura de seguridad de la información, lo que implica también identificar y clasificar los activos de información de la organización.

- Definir y evaluar la metodología para garantizar la integridad, confidencialidad y disponibilidad de la información, determinando la pertinencia de los controles de seguridad de la información de la organización.

- Supervisar la administración de identidades digitales y accesos a la información.

- Supervisar el cumplimiento de los criterios de seguridad de la información definidos por la compañía.

- Asegurar la respuesta ante incidentes de seguridad de la información de la compañía.

- Coordinar con la Dirección de Riesgos la gestión de riesgos de seguridad de la información, implementando medidas preventivas en función de la gestión de vulnerabilidades de los activos de información.

- Comprender e interactuar con disciplinas relacionadas a través de comités, para garantizar la aplicación constante de políticas y estándares en todos los proyectos, sistemas y servicios tecnológicos, incluida la privacidad, la gestión de riesgos, el cumplimiento y la gestión de la continuidad del negocio.

- Mantener contacto con entidades externas -según sea necesario- para garantizar que la organización mantenga una postura de seguridad fuerte y se mantenga al tanto de las amenazas pertinentes identificadas por estos organismos.

- Mantenerse en contacto con el equipo de arquitectura empresarial para crear alineación entre las arquitecturas de seguridad y la de la empresa, garantizando así que los requisitos de seguridad de la información estén implícitos en estas arquitecturas.

- Trabajar en conjunto con el personal de cumplimiento para garantizar que toda la información propiedad, recopilada o controlada por o en nombre de la empresa se procese y almacene de acuerdo con las leyes aplicables y otros requisitos regulatorios globales, como la privacidad de los datos.

- Monitorear el entorno para determinar las amenazas externas, y asesorar a las partes interesadas correspondientes sobre los cursos de acción adecuados.

- Mantener métricas de desempeño de la seguridad de la información, alineadas a la estrategia definida.

- Definir y mantener un programa de formación y concientización en función de los requerimientos de seguridad de la información de la organización, entre los colaboradores y las partes interesadas.

- Supervisar el monitoreo y revisión de eventos de seguridad de la información a nivel de red informática.

- Facilitar una estructura de gobernanza de la seguridad de la información mediante la implementación de un programa jerárquico de gobernanza.

- Trabajar en conjunto con Proveeduría para garantizar que los requisitos de seguridad de la información se incluyan en los contratos mediante la colaboración con las organizaciones de administración y contratación de proveedores.

- Crear y gestionar un programa específico de capacitación en seguridad de la información para todos los funcionarios, proveedores y usuarios de los sistemas, así como establecer métricas para medir la eficacia de este programa de capacitación en seguridad para las diferentes audiencias.

RESPONSABILIDADES

GENERALES

- Preparar y presentar informes sobre su gestión, de forma oportuna y con elevados estándares de calidad, para sus superiores u otra dependencia, según corresponda, con el fin de proveer información confiable para la toma de decisiones.

- Velar, delegar y supervisar el cumplimiento de los indicadores de apetito de riesgo establecidos para los procesos a su cargo, así como las responsabilidades estipuladas en la Política de Gestión Integral de Riesgos y demás normativa aplicable.

- Formular, delegar y supervisar el cumplimiento de las gestiones relacionadas con el cumplimiento normativo de las áreas a su cargo, así como el cumplimiento de las recomendaciones y acciones correctivas resultantes del seguimiento y de las auditorías realizadas.

- Velar por la creación, actualización y el cumplimiento de procedimientos, manuales, formularios, metas, indicadores de gestión y productividad, entre otros; de los procesos a su cargo.

- Conocer y cumplir -de forma estricta- con la normativa aplicable en la realización de sus tareas y reportar a los superiores cualquier tipo de incumplimiento; así como, gestionar el riesgo de cumplimiento asociado a su puesto de trabajo.

- Participar en las actividades de capacitación relacionadas con cumplimiento normativo en general, así como en todas aquellas de interés organizacional que se planifiquen.

- Impulsar la visión transversal de los procesos a su cargo, promoviendo esfuerzos de mejora continua y la optimización de los procesos involucrados, a fin de enfrentar con eficiencia los nuevos retos del mercado y alcanzar los objetivos organizacionales, así como vigilar su cumplimiento.

- Participar activamente en los proyectos de mejora de los procesos a su cargo, establecidos por la organización.

- Ejercer las demás funciones y facultades afines al puesto -en tiempo y forma- que le correspondan, de conformidad con la ley, las políticas, los reglamentos, códigos, programas, disposiciones, manuales y demás normativa aplicable.

(*) *Según los Lineamientos de Atracción y Promoción de la Dirección de Capital Humano*.

Historial de Revisión, Aprobación y Divulgación					
Versión:	**Elaborado por:**	**Revisado por:**	**Aprobado por:**	**Descripción del cambio:**	**Oficio y fecha: (rige a partir de)**
1	PCA	ICH	Gerencia General	Creación	G-02948-2021 (06.07.2021)
2	PCA	MCG	Gerencia General		G-00387-2022 (28.01.2022)
3	LCR	PCA/MCG	AAA		Mediante Memorándum del 29.07.2022
4	VHM	MCG	GG	Actualización de competencias y formato	G-01458-2024 (25.04.2024)
5	KAR	MCG	TVS	Incorporación de categoría de salario integral	Mediante memorándum (23.07.2024)