UNIDAD DE RECLUTAMIENTO, SELECCIÓN Y DESARROLLO ORGANIZACIONAL
SUBDIRECCIÓN DE GESTIÓN Y DESARROLLO DE LAS PERSONAS
HOSPITAL CARLOS VAN BUREN

SOLICITUD DE PROCESO DE SELECCIÓN ABREVIADO PARA SUPLENCIAS/REEMPLAZOS

DATOS DEL PROCESO:

NOMBRE DEL CARGO	Encargado de Seguridad de la Información y Ciberseguridad
TIPO DE LEY	18.834
N° DE VACANTES	01
MODALIDAD CONTRACTUAL	Suplencia
GRADO	8° EUS
REMUNERACIÓN	$2.730.827 (Bruto Mensual)
HORARIO DEL CARGO	Lunes a Jueves 08:00 hrs. a 17:00 hrs. Viernes 08:00 hrs. a 16:00 hrs.
OBJETIVOS DEL CARGO	Proteger los activos de información del Hospital frente a amenazas internas y externas, asegurando la confidencialidad, integridad y disponibilidad de los datos. Esto incluye la implementación de políticas, procedimientos y controles de seguridad, así como la respuesta a incidentes y la promoción de una cultura de seguridad dentro de la Organización, incorporando el uso de Inteligencia Artificial (IA) y Ciencia de Datos como herramientas de apoyo para la detección, prevención y respuesta ante incidentes de seguridad de la información y para apoyo en la gestión del Centro de Responsabilidad (CR) de Gestión de la Información. Administrar los contratos de proveedores que dan servicio al establecimiento en ámbitos de seguridad de la información. Interactuar con las unidades de proyectos TI e infraestructura, Redes y Comunicaciones para garantizar la adhesión a políticas, procedimientos y controles de seguridad vigentes en los proyectos de desarrollo de software, proyectos de infraestructura y en la implantación y/o adquisición de soluciones comerciales, sean clínicas o administrativas.
FUNCIONES DEL CARGO	1. Liderar las iniciativas en materias de seguridad de la información, plantearlas al comité de seguridad de la información, y mantener informado al jefe de servicio, de los acuerdos establecidos en estos escenarios. 2. Velar por la ciberseguridad, y actuar frente a infracciones a la privacidad y amenazas, sus tendencias y escenarios estratégicos que pudieren afectar al Hospital, para asegurar la disponibilidad de servicios y sistemas. 3. Alinear los esfuerzos de las distintas áreas de la Institución, respecto a la protección de los sistemas tecnológicos y a la información contenida en ellos, según los criterios de Ciberseguridad, de forma de mantener una arquitectura de sistemas estandarizada para facilitar su administración. 4. Gestionar internamente el tratamiento de los incidentes que estén vinculados a los activos de información de la institución, identificados y/o reportados tanto por el Ministerio del Interior como por instancias internas del Ministerio y la Red de Salud, efectuando la reportabilidad y el seguimiento adecuado de dichos

	eventos para Dar cumplimiento a la Ley Marco de Ciberseguridad y la Ley de protección y el tratamiento de los datos personales. 5. Apoyar el proceso de sensibilización en materias de ciberseguridad al interior de la institución. Organizando actividades de concientización y capacitación en seguridad para educar a los funcionarios sobre buenas prácticas y comportamientos seguros en pos de generar conciencia en la comunidad funcionaria sobre el buen uso de los recursos tecnológicos. 6. Organizar y presidir el comité de seguridad de la información, que tendrá a su cargo la actualización de políticas y procedimientos, de Ciberseguridad y Seguridad de la Información de la institución, el control de su implementación, y velar por su correcta aplicación asumiendo el rol de líder de los procesos de ciberseguridad en la institución. 7. Coordinar las acciones necesarias para resguardar y asegurar la continuidad del negocio frente a incidentes de Ciberseguridad que permita mantener los servicios operativos, o en su defecto, la más pronta recuperación, durante un incidente de ciberseguridad. 8. Resguardar que se informe adecuadamente a todas las personas naturales y jurídicas que puedan tener acceso a los activos de información de la institución, acerca de las Políticas de Ciberseguridad y Seguridad de la Información vigentes, y en particular sobre las obligaciones que le correspondan en relación a la gestión de incidentes, en correspondiéndole liderar las comunicaciones oficiales durante un incidente de ciberseguridad. 9. Comunicar los incidentes de ciberseguridad de los que tenga conocimiento en ejercicio de sus funciones, al Ministerio del Interior y Seguridad Pública, mediante su notificación al Centro de Respuesta ante Incidentes de Seguridad Informática (“CSIRT”), en el sitio web: https://csirt.gob.cl, en representación del jefe del servicio, en su calidad de autoridad máxima de la institución, dando cumplimiento a las exigencias de la Ley de Ciberseguridad. 10. Establecer puntos de enlace con encargados de seguridad de la información y ciberseguridad, de otros organismos públicos y especialistas externos, que le permitan estar al tanto de las tendencias, normas y métodos en estas materias. 11. Definir políticas y procedimientos de seguridad de la información y ciberseguridad, así como un plan de acción para mitigar riesgos y proteger los sistemas y datos de la organización., materializando las políticas de Estado en temas de Ciberseguridad y adaptarlas a la realidad del Hospital. 12. Apoyar en la identificación, evaluación y gestión de los riesgos de seguridad de la información del Ministerio de Salud, realizando evaluaciones periódicas de vulnerabilidades y amenazas. Implementando controles y medidas para minimizar la exposición a riesgos potenciales y proteger los activos críticos, manteniendo los sistemas de información actualizados y sin vulnerabilidades conocidas. 13. Implementar y mantener los controles de seguridad adecuados para proteger la infraestructura, los sistemas y los datos. Esto puede incluir firewalls, sistemas de detección de intrusos, sistemas de prevención de pérdida de datos y otros mecanismos de seguridad, de forma de mantener un entorno seguro en las habilitantes tecnológicas del Hospital. 14. Evaluar la seguridad de proveedores y terceros con acceso a información sensible de la organización para asegurarse de que cumplan con los estándares de seguridad requeridos, resguardando el cumplimiento de protocolos de seguridad de la información del establecimiento, de MINSAL y del Estado.

	15. Utilizar herramientas de analítica de datos, machine learning e IA para detección de anomalías y patrones de comportamiento sospechoso y para Automatización del análisis de eventos de seguridad, para detectar y mitigar potenciales amenazas de seguridad usando controles automatizados. 16. Liderar y/o Gestionar el desarrollo proyectos del Centro de Responsabilidad de Gestión de la Información que incluyan el uso de IA generativa, agentes IA y modelos extendidos de lenguaje (LLMs) para la gestión clínica y administrativa del establecimiento. 17. Liderar y/o Gestionar el desarrollo proyectos que incluyan el uso de Machine Learning / Deep Learning, incorporar la ciencia de datos como herramienta de apoyo en la gestión de procesos hospitalarios.
FORMACIÓN EDUCACIONAL	- Título Profesional universitario del área de la ingeniería en informática, en sistemas computacionales o similar, otorgado y/o visado por una Universidad Chilena o título extranjero, reconocido y homologado por el Gobierno de Chile. **REQUERIMIENTO MÍNIMO DFL 7** Alternativamente - Título Profesional de una carrera de, a lo menos, diez semestres de duración, otorgado por una Universidad o Instituto Profesional del Estado o reconocido por éste o aquellos validados en Chile de acuerdo con la legislación vigente y acreditar una experiencia profesional no inferior a tres años, en el sector público o privado; o, - Título Profesional de una carrera de, a lo menos, ocho semestres de duración, otorgado por una Universidad o Instituto Profesional del Estado o reconocido por éste o aquellos validados en Chile de acuerdo con la legislación vigente y acreditar una experiencia profesional no inferior a cuatro años, en el sector público o privado.
EXPERIENCIA SECTOR PÚBLICO/SECTOR PRIVADO	Experiencia Requerida (Excluyente): - Al menos 3 años de experiencia laboral en área de informática en instituciones públicas y/o privadas. Experiencia Deseable (No Excluyente): - Al menos 5 años de experiencia laboral en área de informática en instituciones de salud públicas y/o privadas.
COMPETENCIAS	Competencias Transversales: - Compromiso Organizacional - Probidad Administrativa - Respeto y Cordialidad - Vocación de Servicio

	Competencias Específicas: - Trabajo en Equipo - Orientación al Logro de Objetivos - Comunicación Asertiva y Efectiva
CONOCIMIENTOS TÉCNICOS	Conocimiento de normas vigentes de ciberseguridad, como: - NCh-ISO27001:2013: Tecnología de la información - Técnicas de seguridad - Sistemas de gestión de la seguridad de la información – Requisitos. - El Marco Jurídico referido a los Sistemas de Seguridad de la Información (SSI), publicado en el portal del CSIRT del Ministerio del Interior. Conocimiento de Decretos Supremos y Normas Internacionales de Seguridad de la Información y Ciberseguridad: - Leyes relacionadas - Documento del Sistema de Gestión de Seguridad de la Información, disponibles en isalud.minsal.cl. - Ley Nº 20.285, de 2008, del Ministerio Secretaría General de la Presidencia, sobre acceso a la información pública. o Ley N° 19.628, de 2012, del Ministerio Secretaría General de la Presidencia, sobre protección de la vida privada. o Decreto 83, de 2005, del Ministerio Secretaría General de la Presidencia, aprueba norma técnica para los órganos de la administración del estado sobre seguridad y confidencialidad de los documentos electrónicos. Conocimiento en gestión de dirección de proyectos informáticos - Conocimiento en sistemas de información del área de salud. - Conocimiento gestión en salud y administración hospitalaria. - Gestión de Proyectos bajo enfoque del PMI. - Conocimiento y experiencia en procesos hospitalarios. - Conocimiento de Inteligencia Artificial. - Conocimiento de Ciencia de datos.
DEPARTAMENTO Y/O UNIDAD DE DESEMPEÑO AL QUE SE INCORPORARÁ	CR de Gestión de la Información
JEFATURA SOLICITANTE	Sergio Olguín G.
FECHA SOLICITUD	08.04.2026

UNIDAD DE RECLUTAMIENTO, SELECCIÓN Y DESARROLLO ORGANIZACIONAL
SUBDIRECCIÓN DE GESTIÓN Y DESARROLLO DE LAS PERSONAS
HOSPITAL CARLOS VAN BUREN

FECHA DE PUBLICACIÓN	13.04.2026
DIFUSIÓN Y PLAZO DE POSTULACIÓN	13.04.2026 – 24.04.2026
PROCESO DE EVALUACIÓN Y SELECCIÓN DEL POSTULANTE	27.04.2026 – 30.04.2026
FINALIZACIÓN DEL PROCESO	04.05.2026 – 05.05.2026
PUBLICADOR(A)	César Umazábal M.
CARGO	Psicólogo Unidad de Reclutamiento, Selección y Desarrollo Organizacional
FIRMA