CONTENIDO Y PERFIL DE CARGO

|  |  |  |  |
| --- | --- | --- | --- |
| NOMBRE DEL CARGO/FUNCIÓN | DEPENDENCIA | UNIDAD DE TRABAJO Y ESTABLECIMIENTO | **GRADO** |
| Encargado/a de Infraestructura de Servidores | Jefatura Unidad de Ciberseguridad | Departamento TIC | 15º |

|  |
| --- |
| CONTENIDO DEL CARGO |
| **OBJETIVO O PROPOSITO DEL CARGO** |
| Administrar la infraestructura de servidores del Hospital Provincial de Ovalle para gestionar, monitorear y resguardar el uso de los recursos de procesamiento y almacenamiento disponibles, velando por el correcto funcionamiento de los sistemas informáticos y de información, a través de la implementación de procedimientos documentados que se alineen con las mejores prácticas en ciberseguridad para la continuidad de las operaciones, la capacidad de resiliencia y las políticas de seguridad de la información definidas por el establecimiento. Además, prestará apoyo en labores de soporte a usuarios, implementación de controles de seguridad informática, la gestión y el mantenimiento de las herramientas de seguridad que administra la unidad. |
| **FUNCIONES PRINCIPALES PARA DESEMPEÑAR EL CARGO:** |
| |  |  | | --- | --- | | **N°** | **FUNCIONES** | | **1** | Supervisión de la sala de servidores para mantener condiciones adecuadas de operación y seguridad. | | **2** | Administrar plataformas de virtualización On-Premise y Cloud. | | **3** | Administrar Servidores Institucionales a nivel de sistema operativo para la provisión de servicios en red. | | **4** | Definir, documentar y aplicar procedimientos seguros para la administración y operación de servidores y servicios TIC. | | **5** | Documentar y mantener registros actualizados sobre el estado y configuración de los activos de información bajo su administración. | | **6** | Monitorear la seguridad y la operación de servidores, servicios y aplicaciones del hospital. | | **7** | Realizar mantenimiento preventivo y correctivo de los activos y sistemas de información, asegurando la continuidad y calidad del servicio, mediante el uso de herramientas tecnológicas. | | **8** | Implementar herramientas de seguridad especializadas en servidores. | | **9** | Mantener actualizado y parchado el software operacional administrado por la unidad de acuerdo con los procedimientos internos. | | **10** | Participar en la respuesta a incidentes de ciberseguridad. | | **11** | Apoyar en la capacitación y concientización del personal del hospital. | | **12** | Trabajar colaborativamente con la Unidad de Desarrollo de Software en tareas de DevOps. | | **13** | Proporcionar atención a los usuarios para brindar soporte técnico remoto y presencial. | | **14** | Gestionar el acceso seguro a recursos compartidos en red. | | **15** | Subrogar al jefe de la unidad. | | **16** | Realizar otras funciones que la jefatura asigne de acuerdo con su ámbito de competencia. |   < |

|  |
| --- |
| **REQUISITOS ESPECIFICOS PARA EL DESEMPEÑO DEL CARGO/FUNCION:** |
| **REQUISITOS EDUCACIONALES EXIGIBLES**: |
| - 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. |
| **REQUISITOS FORMALES (DESEABLES):** |
| - Título de Ingeniero en Informática, Ingeniero en Telecomunicaciones, Ingeniero en Ciberseguridad, Ingeniero en Computación o Ingeniero en Conectividad y Redes.  **Experiencia:**  - Experiencia en instituciones de salud hospitalaria en el área de tecnologías de la información y las comunicaciones. (1 año)  **Capacitaciones**  Diplomados:  - Diplomado en Ciberseguridad, Seguridad Digital o Seguridad Informática.  Cursos:  - Capacitación en Administración de Servidores, Servicios de Infraestructura de TIC.  - Capacitación en Sistemas Virtualizados o Virtualización.  - Capacitación en Machine Learning.  - Capacitación en fundamentos de Ciberseguridad, Seguridad Informática, Seguridad Cibernética.  - Capacitación en Seguridad para Terminales, Sistemas Operativos.  - Capacitación en Seguridad Defensiva o Blueteam.  - Capacitación en Lenguaje de Programación Python.  - Capacitación en pruebas de software, testing o QA para aplicaciones web.  - Capacitación en normativa y estándares de Seguridad de la Información y Ciberseguridad. |

|  |
| --- |
| **COMPETENCIAS** |
| **COMPETENCIA TÉCNICAS:** |
| **Conocimiento en:**  **-** Plano de administración de dispositivos e infraestructura.  **-** Fundamentos de Ciberseguridad.  **-** Virtualización.  **-** Seguridad en dispositivos finales.  **-** Seguridad defensiva.  **-** DevOps.  **-** Normativa y Legislación en Ciberseguridad sector salud. |

|  |  |  |
| --- | --- | --- |
| **COMPETENCIAS DIRECTIVAS:** | | |
| **DESCRIPCIÓN** | **Nivel Dominio Requerido** | |
| 1. Liderazgo de Equipos | 3 | |
| 2. Orientación a la eficiencia y calidad del trabajo | 3 | |
| **COMPETENCIA TRANSVERSALES:** | | |
| **DESCRIPCIÓN** | | **Nivel Dominio Requerido** |
| 1. Trabajo en Equipo | | 3 |
| 2. Comunicación Eficaz | | 4 |
| 3. Orientación y Atención al Usuario | | 3 |
| 4. Responsabilidad | | 4 |
| 5. Iniciativa y proactividad | | 3 |