POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

IPC CENTRO DE SALUD INTEGRAL S.A. es un centro médico especializado en salud ocupacional y exámenes médicos ocupacionales (EMO) para empresas, cumpliendo con las normativas vigentes. Conscientes de la importancia de la información como un activo fundamental para la operación y prestación de nuestros servicios, establecemos la presente Política del Sistema de Gestión de Seguridad de la Información (SGSI).

Esta política se aplica a todos los activos de información gestionados por IPC SALUD S.A., incluyendo datos, sistemas de información, infraestructura tecnológica y gestión humana.

En IPC Salud, asumimos los siguientes compromisos:

1. Seguridad de la información. Preservar la confidencialidad, integridad y disponibilidad de la información mediante medidas organizativas, humanas, físicas y tecnológicas proporcionales al riesgo. Prevenir el acceso y la divulgación no autorizados, las alteraciones indebidas y la pérdida o destrucción de información.
2. Ciberseguridad. Proteger los sistemas, redes, aplicaciones y datos frente a amenazas digitales que puedan comprometer la atención y la información. Prevenir, detectar, responder y recuperarse de ataques informáticos mediante controles de acceso, autenticación reforzada, actualizaciones y protección contra programas maliciosos, según los riesgos identificados.
3. Protección de la privacidad. Respetar la vida privada y los derechos de las personas sobre sus datos personales. Tratar únicamente los datos necesarios para finalidades informadas y legítimas, con base jurídica válida y consentimiento cuando sea exigible. Facilitar los derechos de acceso, rectificación, cancelación y oposición.
4. Cumplimiento de requisitos. Cumplir con todas las leyes, regulaciones y estándares aplicables en materia de seguridad de la información, incluyendo la normativa ISO/IEC 27001 y las disposiciones legales peruanas relacionadas con la protección de datos y seguridad.
5. Riesgos y objetivos. Evaluar y tratar los riesgos de seguridad, ciberseguridad y privacidad, con responsables y aceptación del riesgo residual por sus propietarios. Mantener el plan de tratamiento y la declaración de aplicabilidad.
6. Incidentes y continuidad. Establecer canales para reportar oportunamente eventos e incidentes físicos o digitales. Evaluarlos, contenerlos, documentarlos y recuperar los servicios, preservando las evidencias. Notificar a autoridades y personas afectadas en los supuestos y plazos legales.
7. Responsabilidades y recursos. Definir y comunicar autoridades y responsabilidades, asignar recursos y capacitar al personal en seguridad de la información, ciberseguridad y privacidad. Designar al Oficial de Datos Personales cuando resulte exigible, conforme a la normativa y al cronograma aplicable.
8. Evaluación y mejora. Revisar objetivos, requisitos y eficacia de los controles mediante seguimiento, auditorías internas y revisión por la dirección. Corregir no conformidades, verificar las acciones correctivas y aplicar las lecciones de los incidentes para mejorar continuamente el SGSI.

IPC CENTRO DE SALUD INTEGRAL S.A. requiere el continuo compromiso y responsabilidad de los/as colaboradores/as para cumplir con la presente política.

Lima, 03 de Agosto 2026.

SARA PAJARES QUISPE
Gerente General