Fecha: 25 de enero del 2013
Razón social: Sociedad Comercializadora de Insumos y Servicios Médicos S.A.S 'SOCIMÉDICOS S.A.S´
NIT: 900342064 – 3
Dirección:

- **Clínica San Rafael sede Megacentro /** Cra 19 N°12-32, sector Pinares
- **Clínica San Rafael sede Megacentro PH /** Cra 18 # 12-75 Torre 2 piso 13, sector Pinares
- **Clínica San Rafael sede Cuba /** Cra 25 N° 74 ª-87, Barrio Rafael Uribe II, sector Cuba
- **Clínica San Rafael sede Icono /** Avenida Juan B. Gutiérrez N° 17-55 ICONO (consultorios 306, 403, 507), sector Pinares
- **Clínica San Rafael sede Oval Médica /** Avenida Juan B. Gutiérrez N° 18-60 OVAL MÉDICA (consultorios 703, 901, 902, 903, 904, 905), sector pinares
- **Clínica San Rafael sede Alamos /** Calle 11 N° 24-30, sector Alamos

POLÍTICA DE SEGURIDAD INFORMÁTICA

Las Políticas de Seguridad establecidas en este manual regirán para todos los miembros de la institución **CLÍNICA SAN RAFAEL - SOCIMÉDICOS S.A.S y sus sedes**, deberán ser acatadas por todas aquellas personas que en el ejercicio de sus labores interactúen con los servicios, recursos informáticos y comunicaciones de la clínica tanto en forma directa como indirecta.

Toda persona que pertenezca a la institución asume cumplir y respetar al pie de la letra el manual de políticas de seguridad de la clínica, el cual implica lo siguiente:

- De acuerdo a la labor ejercida en la clínica, apoyándonos en turnos rotativos las 24 horas del día y 365 días del año, a todo empleado se suministrará un usuario para acceder en equipos informáticos y red, este usuario es de uso único para el equipo y de uso en común dependiendo en el área de trabajo donde desempeñe su labor, el empleado se hace responsable de su uso durante su jornada laboral.
- Solo en casos excepcionales para labores de personal administrativo y directivo el usuario será único e intransferible y la responsabilidad es personal de salvaguardar informático asignado.
- Aceptará todas las condiciones de confidencialidad de la empresa.
- Todos los usuarios se hacen totalmente responsables del uso de las aplicaciones una vez se hayan autenticado con su user (usuario) y password (contraseña).
- Se recomienda bloquear el equipo al ausentarse del puesto de trabajo.
- Hará uso adecuado de los bienes informáticos y de la información de la institución.
- Cumplirá al pie de la letra las directrices del Manual de Políticas de Seguridad.
- Se considerará como grave el robo, daño o divulgación de la información de la institución.
- El empleado deberá reportar en todo momento al área de sistemas si hay algunos riesgos reales o potenciales sobre los equipos informáticos.
- El empleado se hace completamente responsable de los equipos y accesorios informáticos que se le entreguen o asignen para desarrollo de su labor en la institución. (equipos portátiles, de escritorio, módems, unidades de almacenamiento externas, etc.)
- El empleado se hace responsable de la persona ajena a la institución que entre bajo su autorización.
- Todos los bienes informáticos solo podrán salir de la institución previa notificación a Gerencia y bajo autorización por escrito de responsable directo.
- El área de trabajo siempre debe estar limpia de polvo y libre de humedad para evitar desastres.
- Está terminantemente prohibido el consumo de bebidas y comida en el área laboral.

- El daño del equipo por negligencia, maltrato o descuido será únicamente responsabilidad de la persona a la cual fue asignado el equipo informático.
- Únicamente está autorizado personal del Área de Sistemas a instalar o desinstalar aplicaciones en los equipos de la institución previa justificación y autorización por Gerencia.
- Si el empleado lo requiere solicitará capacitación para manejo de software específico de la institución y el mal uso del mismo será única y exclusivamente responsabilidad del empleado.
- Queda terminante prohibido la manipulación física (apertura) de equipos de la institución a personal que sea ajeno al Área de Sistemas.
- Toda la información más importante deberá guardarse en una carpeta asignada a su usuario almacenada en una unidad de red para salvaguardar posible pérdida de datos en el equipo físico.
- El uso de cuenta de correo asignada a cada empleado es privada e intransferible, se prohíbe terminantemente el uso de cuentas de correos ajenos a la institución.
- Toda la información enviada y recibida a través de la cuenta de correo de la institución es propiedad de la misma.
- Si se sospecha del envío de información que comprometa la seguridad de la institución, la dirección se reserva el derecho de auditar mensajes y archivos adjuntos enviados y recibidos a través de la cuenta de correo de la institución.
- El empleado utilizará la cuenta de correo únicamente para enviar y recibir información y archivos de acuerdo a su labor en la institución.
- La alteración de la configuración en las aplicaciones es responsabilidad del empleado.
- Si se sospecha de alteración en la configuración del software no hecha por el empleado deberá notificarlo al Área de Sistemas.
- El acceso a internet está restringido, solo se podrá acceder previa autorización con justificación por Gerencia o responsable inmediato, siempre y cuando sea indispensable para la labor del empleado en la institución.
- El acceso a internet libre es exclusivo para la labor del empleado en la institución, no se permite el acceso a internet para beneficio personal.
- Queda prohibido la instalación de software ajeno a la institución en equipos informáticos.
- Los empleados de IPS CLÍNICA SAN RAFAEL no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red de la entidad, sin la autorización del Área de Sistemas.
- Es obligación del Área de Sistemas informar a los empleados sobre el Manual de Políticas de Seguridad en la Información.