INTRODUCCIÓN

La ESE Hospital San Vicente de Paul de Santuario Risaralda, busca garantizar a nuestros usuarios-clientes-comunidad, que la información recopilada de las atenciones realizadas, cuenta con mecanismos para su protección y confidencialidad, bajo criterios éticos definidos en la normatividad vigente.

Alcance: La política de confidencialidad y privacidad es transversal a toda la Empresa, buscando que todos nuestros servidores sean guardianes de la información y privacidad de nuestros usuarios.

POLÍTICA

En la E.S.E Hospital San Vicente de Paúl de Santuario Risaralda es política institucional, garantizar al usuario ética profesional y respeto por la información correspondiente a la atención prestada y su intimidad, estableciendo procesos que respondan a la normatividad vigente y a sus derechos; teniendo herramientas para la protección y custodia de los registros clínicos e infraestructura que facilite su comodidad; con personal capacitado y motivado para establecer un vínculo con el usuario, permitiéndole sentir como propias sus necesidades; adicionalmente es compromiso institucional garantizar los recursos financieros necesarios para la el mejoramiento tecnológico e infraestructura requerida para que a los servidores públicos se les facilite el cumplimiento de las políticas.

A. POLÍTICAS DE CONFIDENCIALIDAD:

1. Al momento de ingresar los usuarios al servicio de hospitalización se les debe interrogar sobre a quiénes se les puede brindar información sobre su estado de salud.
2. Sólo el médico debe brindar información sobre el estado de salud de los usuarios.
3. Al archivo clínico solo pueden ingresar los funcionarios que laboran en ésa área.

4. Todos los registros concernientes a la atención clínica de los usuarios, deben ser archivados en la historia clínica.
5. La historia clínica es de propiedad del usuario, la ESE es responsable de su custodia y conservación: cuando el usuario solicite una copia de su historia debe venir personalmente con su documento de identidad o enviar una autorización.
6. El acceso a las historias clínicas con fines administrativos debe estar normalizado, estableciendo los controles necesarios que garanticen su confidencialidad.
7. La historia clínica solo puede ser conocida por terceros con previa autorización del usuario o en los casos previstos en la ley: fines administrativos (auditorías médicas), investigaciones de salud pública y procesos legales requeridos por autoridad judicial competente.
8. Se deben garantizar procesos de respaldo y restauración de la información.
9. Establecer procesos que garanticen restricciones de acceso a la información a los servidores públicos, de acuerdo a sus funciones.
10. No se deben realizar conversaciones sobre el estado de salud de los usuarios en los pasillos de la ESE o lugares públicos.
11. Las consultas con otros profesionales para aclarar un diagnóstico, no deben realizarse delante de otros usuarios o funcionarios.
12. Los resultados de exámenes de Laboratorio deben ser consignados directamente en la historia clínica. Cuando el usuario los solicite, éste debe reclamarlos directamente con su documento de identidad o en su defecto, diligenciar una autorización para que otra persona los pueda reclamar.
13. El personal encargado de las actividades a nivel extramural, es responsable de la custodia de las historias clínicas, las cuales deben ser devueltas a la institución luego de la atención al usuario.
14. En los casos en los que el personal del hospital, de tipo administrativo o asistencial requieran acceder a las historias clínicas consignadas en el archivo histórico de la institución deben hacerlo con previa autorización y deben llenar el formato para el acceso a archivos históricos, central o de gestión.
15. Todos los funcionarios y contratistas deberán firmar la cláusula y/o acuerdo de confidencialidad definido y este deberá ser parte integral de cada uno de los contratos. Este requerimiento también se aplicará para los casos de

contratación de personal temporal o cuando se permita el acceso a la información y/o a los recursos de la institución a personas o entidades externas.

B. POLÍTICAS DE PRIVACIDAD

1. Adecuar la estructura física para facilitar la privacidad y el respeto por la dignidad de cada usuario.
2. La atención a los usuarios no se debe interrumpir con llamadas por celular, telefónicas o conversaciones con otros compañeros, el usuario es nuestra prioridad.
3. Cuando se esté brindando atención a un usuario, se debe solicitar permiso para el acceso de otras personas al consultorio o habitación si está hospitalizada.
4. La atención a los usuarios debe realizarse en los consultorios o áreas definidas para ello.
5. En las diferentes dependencias se debe atender un usuario a la vez, brindándoles información para que se respeten los turnos correspondientes, garantizando privacidad.
6. Sensibilizar a los usuarios sobre el respeto por la privacidad de las otras personas.
7. Ofrecer al usuario los implementos necesarios para que se sienta cómodo en la atención (batas y baño para cambiarse), cierre la puerta del consultorio o área para atender a cada usuario.

C. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LOS RECURSOS INFORMÁTICOS

Complementando lo anterior, los funcionarios de la ESE Hospital San Vicente de Paúl deben velar por la información que se almacena en los recursos informáticos, por lo cual lo cual se deben seguir las siguientes recomendaciones que son de obligatorio cumplimiento:

1. Está prohibido intentar violar los controles de seguridad que se implementen para proteger los recursos informáticos.

2. Se deben usar los activos informáticos con previa autorización, a menos que sean parte de las funciones asignadas.
3. No se debe intentar evadir o violar la seguridad o autenticación que se han establecido en los diferentes sistemas de información de la entidad.
4. Las contraseñas, firmas digitales o dispositivos de autenticación son intransferibles, a menos que se pida previa autorización con la directiva de la entidad.
5. No se debe acceder a servicios informáticos haciendo uso de cuentas o medios de autenticación de otros usuarios sin previa autorización de la directiva de la entidad.
6. Solo el área de sistemas de información de la entidad está autorizado para instalar y configurar software en los activos informáticos.
7. Está prohibido usar, distribuir y ejecutar software malicioso que cause daños, molestias, alteraciones en la ejecución de las labores o que vulnere la seguridad de los dispositivos informáticos de la entidad.
8. No se debe extraer sin previa autorización datos, información, material, equipos informáticos, o elementos de los recursos informáticos de la entidad sin autorización previa.
9. El uso del internet debe ser sólo con fines laborales, y se debe evitar la reproducción de material obsceno, pornográfico, difamatorio o que implique una amenaza tanto para la entidad, funcionarios, usuarios o recursos informáticos.
10. Los mensajes de correo electrónico que salen de la entidad o son divulgados internamente no pueden ser contrarios a los lineamientos y decisiones tomadas por la dirección de la entidad.
11. En los recursos informáticos asignados no se deben almacenar aplicaciones, programas, archivos, videos o audios que no se relacionen con el quehacer de cada puesto de trabajo o dependencia.
12. Cada funcionario tiene la responsabilidad de velar por la protección de los datos, contraseñas y los recursos informáticos asignados para la función de sus labores, y deben reportar al área de sistemas de información cualquier irregularidad detectada.
13. Se establecerá un procedimiento para hacer copias de seguridad.