POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

Prosvisalud se compromete a garantizar la seguridad de la información conforme a la Ley 1581 de 2012 y normativas afines. A través de convenios de confidencialidad e imparcialidad, se asegura el cumplimiento de estas normativas en las relaciones con proveedores y contratistas que contribuyan a los servicios de salud y certificación de la IPS.

En el ámbito de los sistemas de información, Prosvisalud promueve la ética y la transparencia, buscando mejorar la idoneidad en el uso de tecnologías de la información y gestión documental:

- Todas las estaciones de trabajo y computadoras de usuario final deben tener instalado software de protección contra virus.
- Contar con un inventario detallado de la infraestructura de Hardware y software de la Institución, acorde con las necesidades existentes de la misma, así como de los documentos que se conservan físicamente
- Documentar el programa anual de mantenimiento técnico preventivo de todos los equipos informáticos de la Institución.
- El proveedor de sistemas informáticos establece las configuraciones automatizadas para que los usuarios guarden toda su información en los discos de red respectivos y necesarios y que puedan facilitar las copias de seguridad (backup) correspondientes, procurando copias de calidad que sean de ayuda total cuando se necesiten.
- Está prohibido instalar y/o descargar juegos, videos, música y aplicaciones de páginas del Internet, que no guarden relación con la actividad laboral de la IPS.
- Está prohibido tener en los discos de Red archivos que no tengan o guarden relación con la institución tales como música, fotos, videos, ejecutables, entre otros.

- Garantizar acceso restringido a los archivos clínico y administrativo en donde se custodie información de la institución.
- Contar con un plan de emergencia, conservación, seguridad y custodia de la información física y electrónica, que facilite la continuidad en la prestación de los servicios de salud y la ejecución de las actividades administrativas al momento de presentarse un evento.
- Los usuarios finales deberán revisar y responder día a día todos los correos electrónicos internos como externos relacionados con las actividades de la Institución.
- Todas las informaciones institucionales se deben manejar exclusivamente a través de los correos internos que dispone la organización para tal fin.
- No se puede transferir a terceros ningún tipo de información de la empresa, a menos de que se cuente con autorización expresa por parte del jefe inmediato.
- Se debe guardar la información de trabajo en los discos de red asignados por usuario, garantizando así la integridad de la información.
- Todos los usuarios de los sistemas de información deben crear una contraseña privada, con la finalidad de acceder a los datos, servicios y programas de su equipo, la cual no deben compartir.
- Los colaboradores se deben comprometer a no hacer uso indebido de la información institucional que manejan.
- El personal encargado de sistemas se asegurará de coordinar con los encargados de las áreas, las páginas de Internet a las que puede tener acceso al igual que el personal bajo su cargo, bloqueando aquellas páginas que no sean relevantes para el desempeño de las funciones.
- El personal de sistemas deberá monitorear el acceso de las páginas de internet por parte del personal e informar cualquier violación de acceso, vía correo electrónico a Gerencia.
- Está prohibido la transmisión y/o, descarga de material obsceno o pornográfico, o que contenga amenazas o cualquier tipo de información que atente contra la moral y buenas costumbres del personal.
- Todas las áreas de procesamiento de información y que se usen para mantener estos recursos deben ser protegidas con controles físicos y apropiados de acuerdo al tamaño, la complejidad de las operaciones, la

criticidad y sensibilidad de los sistemas que operan en ellas. El acceso físico a estas áreas debe ser restringido y solo permitir el acceso a personal autorizado. Los visitantes autorizados deben ser supervisados y el ingreso y salida debe quedar registrada en la planilla respectiva.

- Capacitar y retroalimentar permanentemente a todo el personal en el tema de gestión del riesgo informático, privacidad, confidencialidad y protección de datos.
- Garantizar control sobre el acceso externo a la red de datos de la IPS.

Revisada: 05 / 09 / 2024

CONSTANZA VIVIANA TORRES CANO
CC 30239704
GERENTE