# POLITICAS SEGURIDAD DE LA INFORMACIÓN

# ENDOCIRUJANOS SAS

El presente documento tiene como propósito proteger la información de la compañía plasmada en los sistemas de información y archivo físico con el fin de minimizar los riesgos de posibles desastres de tipo físico (Incendios, robos, terremotos) o informáticos (Virus, malware, spam, etc.) en donde todos los funcionarios de ENDOCIRUJANOS serán los responsables de la misma cumpliendo con las políticas mínimas de seguridad de la información.

Para cumplir con el objetivo anterior, es necesario cumplir con las siguientes políticas a saber:

1. Todo funcionario es responsable del software que utiliza en su equipo asignado, motivo por el cual no sé, debe instalar software adicional diferente al que es utilizado por la compañía; El funcionario que lo haga será hará responsable de los acontecimientos que puedan suscitar por violar esta norma. El software básico que debe tener todo equipo de cómputo de nuestra compañía es:

- Paquete de oficina Libre Office (software por el cual generamos documentos, hojas de cálculo, correo electrónico, etc.)
- Antivirus Eset Endpoint Security
- Visualización de archivos en formato pdf. Acrobat reader
- Aplicativo contable y financiero CGUNO
- Navegadores de internet chrome y mozilla.
- Aplicaciones de la DIAN, SUPERSALUD, SIC y otros.
- Compresor de información WINRAR(free)

En caso que un funcionario de la compañía requiera de un software adicional, que no esté estipulado en este numeral, debe informar al área de informática para evaluar desde el punto de vista económico y tecnológico, la posibilidad de ser instalado.

2. El correo que se asigna a cada usuario según sus funciones es de carácter corporativo. Por lo anterior se prohíbe el uso del mismo con fines personales, con el fin de evitar ataques informáticos por este medio. Si por algún motivo, le llegare a ingresar correos electrónicos de dudosa procedencia, **por favor no abrir e informar al área de informática.**
3. Dar un adecuado uso al servicio de internet. Evitar visitar páginas de dudosa procedencia para evitar posibles ataques informáticos que puedan perjudicar la

información de la empresa. No navegar en redes sociales como Facebook, youtube, instagram, etc

4. El funcionario realizara copia de seguridad de su información en su computador asignado de todo lo registrado en el corporativo, adicional a la copia del área de informática. Para este fin se realizara en cada equipo una función automática para que se haga dicha copia. Es deber del funcionario revisar que la copia se esté realizando correctamente en caso contrario debe informar al área de informática.
5. Todos los usuarios deben ser conscientes de la importancia de la información que generan, por tanto es responsabilidad de cada usuario que su información, se esté almacenando en el lugar indicado por el área de sistemas para su correspondiente copia de seguridad. El área de sistemas no se hará responsable de la información que este por fuera de lo estipulado en las políticas de seguridad
6. Los puertos USB de los computadores de la compañía (Portatiles y escritorio), No estará deshabilitados para evitar el uso de las memorias. Cada área de la compañía debe contar con un equipo que permita la utilización de los mismos, siempre y cuando sea un trabajo corporativo. Prohibido la utilización de estos dispositivos de uso personal para labores diferentes a la de la compañía como usb o dvd utilizadas para trabajos , hojas de vida, etc que son introducidas en café internet, universidades y demás equipos diferentes a las de ENDOCIRUJANOS
7. Los funcionarios deben de Informar al área de informática en caso de que se encuentre anomalías en su equipo de trabajo (Computador lento, mensajes extraños, etc).
8. **Copias de seguridad**: Se realiza a diario copias de seguridad de la información al aplicativo contable CGUNO en el NAS y día de por medio se realizara copia de la carpeta FINANCIERO, CORPORATIVO Y ENDORIPS la cual contiene documentos y demás información generada por los usuarios de la red. Se realizara una copia semanal (Día Viernes) de la información en un disco duro externo el cual debe salir de nuestras instalaciones con el fin de salvaguardar la información de un desastre físico (incendio, terremotos, asaltos a la propiedad, etc.).
9. El servidor de comunicaciones será configurado para denegar accesos a ciertas páginas en su mayoría sociales con el fin de evitar infiltración de software no deseado como spam, virus, malware, etc.
10. Todos los equipos cuentan con Eset EndPoint Security, aplicativo de seguridad que permite detectar y eliminar software malicioso que puede contener virus, spam, malware, etc. Por lo anterior cualquier mensaje que arroje este software en la pantalla del equipo, por favor informar al área de sistemas.

11. El servicio de Wifi será exclusivo para navegación en equipos portátiles de clientes o proveedores.
12. Cada que termine los funcionarios su labor diaria favor verificar el apagado de sus equipos de cómputo e impresión.
13. De acuerdo a la Ley 1581 de 2012 y el decreto 1377 de 2013 correspondiente al habeas data y protección de datos y estipulado en los contratos laborales, se prohíbe a los funcionarios de la compañía, revelar o copiar información relacionada con pacientes o funcionarios sin una expresa orden de carácter judicial o jefe inmediato.
14. La información registrada en el área de archivo es de uso exclusivo de la clínica, por lo anterior si algún funcionario requiere información del archivo debe acudir al encargado de este proceso para generar un documento en donde se especifique los datos necesarios para el uso del mismo.
15. En caso de caída del SIIS, aplicativo clínico existe la aplicación propia ENDORIPS como plan de contingencia para mitigar el evento adverso. Este debe estar instalado en los equipos de admisiones y procedimientos.
16. Implementación de formato de ley 1581 para pacientes, proveedores y empleados que deberán ser almacenados en forma digital.