**POLITICAS DE USO DE LOS RECURSOS TECNOLOGICOS**



HOSPITAL DEPARTAMENTAL SAN RAFAEL 2017-2018

El Hospital Departamental San Rafael, provee a sus colaboradores un sistema informático y el equipamiento correspondiente para el cumplimiento de las tareas a su cargo. En consecuencia, el acceso al sistema informático y al uso de internet o de intranet provisto por el hospital posee las características de una herramienta de trabajo.

Se encuentra prohibido a todo el personal y se considera uso indebidodel sistema informático de la Empresa:

1. Utilizar para fines personales y/o extra laborales el sistema informático y el equipamiento puesto a su disposición.

2. Utilizar programas sin el soporte legal, ni licencia correspondiente o incorporar a su computadora programas no adquirido legalmente por la Empresa.

3. Incorporar programas sin autorización previa escrita delHospital, y/o con contenidos no correspondientes al sistema informático de la Empresa.

4. Vulnerar de cualquier forma y con cualquier medio la confidencialidad de la información existente en el sistema del Hospital.

5. Extraer copias de la información de cualquier tipo que obra en el sistema delhospital sin previa autorización escrita.

6. Enviar e-mails y/o "chatear" por motivos ajenos alHospital y a sus tareas, ya sea con terceros (incluyendo amigos o familiares) o con personal de la Empresa.

7. La asignación de una clave personal de acceso al trabajador no le otorga derecho alguno a la utilización privada del sistema informático o al correo asignado para su puesto. En consecuencia, respecto de la correspondencia electrónica, se prohíbe el envío o recepción de e-mails por cuestiones personales.

8. El personal debe hacer uso adecuado de los recursos informáticos (PC, impresoras, programas, correo, etc.) y el personal de sistemas debe monitorear que se cumpla esta política. Además, todo el personal deberá informar a sistemas sobre cualquier falla, desperfecto o mal uso del equipo de cómputo, para su adecuado seguimiento.

9. Todo el personal tendrán una cuenta de correo electrónico interno, que les permite recibir y enviar información indispensable para sus actividades. Estas cuentas de correo, sólo son para uso interno, no tienen la capacidad de enviar correos públicos.

**Sobre la seguridad de la información**

10. Los equipos deberán contar con salvapantallas protegido por contraseña con un tiempo de espera de 1 minuto para evitar accesos no autorizados.

11. Todos los accesos a los programas principales estarán protegidos mediante un mecanismo de usuario y contraseña así como permisos de acceso. De igual forma, las sesiones de Windows personales estarán protegidas con contraseña.

12. Todos los archivos que viajen por correo y que contengan información sensible deberán estar comprimidos con contraseña de uso interno como medida de seguridad de información.

13. Todos los equipos asignados a los conectores/gestores tendrán deshabilitados los accesos a puertos USB, CD o Diskettes. Esta medida tiene 3 objetivos:

Evitar ataques de virus en los equipos y el servidor.

Evitar extracciones no autorizadas.

Evitar la carga de archivos ajenos a la labor de gestión.

14. Los equipos autorizados para el uso de dispositivos de almacenamiento externos están supervisados por coordinación y por el área de sistemas, para la entrada y salida de información.

15. A todos los equipos se les realizará una revisión de virus por lo menos cada mes, que incluye las siguientes actividades.

Actualizar su base de firmas de virus (actualización de la lista de amenazas)

Búsqueda de virus (análisis del equipo)

Eliminación de virus si fue detectado.

16. En caso autorizado de memorias USB y discos, es responsabilidad del usuario hacer uso del antivirus antes de copiar o ejecutar archivos para que los equipos no sean infectados. Además los usuarios pueden pedir apoyo al departamento de sistemas para el uso de antivirus.

**Sobre el mantenimiento y buen uso de la infraestructura**

17. Todos los equipos deberán presentar las últimas actualizaciones de Windows, parches de seguridad y antivirus instalado.

18. Los equipos de toda la agencia deberán de estar conectados a un regulador de corriente, como medida de prevención de variaciones de electricidad.

19. Si se presentara una suspensión de servicio eléctrico y el servidor solo se sostuviera con el no-break, se tendrán que apagar primero todos los equipos de la hospital y posteriormente el servidor.

20. El servidor y la máquina principal del área administrativa deberán conectarse a un equipo no-break para evitar la pérdida de información en los equipos por variaciones o fallas de energías.

21. Una vez al año se realizara una revisión en la red para detectar desperfectos y dar así mantenimiento .

22. Periódicamente, por espacio de 6 meses, se realizará una limpieza física a toda la infraestructura de equipo de cómputo por parte del personal de sistemas.Previo a una programación el usuario deberá entregar el equipo para su limpieza en el horario programado.

23. Toda actividad elaborada por el equipo de sistemas deberá de estar debidamente documentada para darle seguimiento y que sirva como evidencia en los procesos de auditoría interna.

La desobediencia de cualquiera de estas normas será considerada como grave incumplimiento laboral.

Comité de Gobierno en Línea TIC