La Clínica Sagrado Corazon está comprometida con establecer medidas de índole técnica necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (voz y datos)) y de las personas que interactúan haciendo uso de los servicios asociados a ellos.

Luego de realizar un análisis de riesgos y de vulnerabilidades en las dependencias de la clínica se determina que los Administradores de Tecnología de Información de la Clínica Sagrado Corazón son los responsables velar por una adecuada utilización de equipos de cómputo, sistemas de información, redes informáticas, procesamiento de datos e información y la comunicación.

Esta política es aplicable a todos los empleados, contratistas, consultores, eventuales y otros empleados de la clínica, incluyendo a todo el personal externo que cuente con un equipo conectado a la red de igual manera aplica para todo el equipo y servicios propietarios o arrendados que de alguna manera tengan que utilizar local o remotamente el uso de la Red o recursos tecnológicos de la clínica así como de los servicios e intercambio de archivos y programas.

NATASHA MOLINA VELEZ
GERENTE GENERAL

1. OBJETIVOS:

- Dotar de la información necesaria a los usuarios de las normas y mecanismos que deben cumplir y utilizar para proteger el hardware y software de la red, así como la información que es procesada y almacenada en estos.
- Planear, organizar, dirigir y controlar las actividades para mantener y garantizar la integridad física de los recursos informáticos, así como resguardar los activos de la clínica.

Los objetivos que se desean alcanzar luego de implantar las Políticas de Seguridad son los siguientes:

- Establecer un esquema de seguridad con perfecta claridad y transparencia bajo la responsabilidad de sistemas de información en la administración del riesgo.
- Comprometer a todo el personal de la clínica con la seguridad y en la agilidad en la aplicación de los controles convirtiéndolos en interventores del sistema de seguridad.

2. VIGENCIA:

Todo empleado es responsable del cumplimiento de los estándares, directrices y procedimientos de control de acceso, así como también notificar a su nivel jerárquico superior, cuando por algún motivo no pueda cumplir con las Políticas de Seguridad indicando el motivo por el cual no le es posible apegarse a la normativa de seguridad. Cabe destacar que este nivel de responsabilidad va a ser conocido por las diferentes áreas de la clínica quienes serán las garantes de que esta información sea conocida por cada integrante de área.

La documentación presentada como Políticas de Seguridad entrará en vigencia desde el momento en que sean aprobadas por la Gerencia.

Esta normativa deberá ser revisada y actualizada conforme a las exigencias de la clínica o en el momento en que haya la necesidad de realizar cambios sustanciales en la infraestructura tecnológica.

3. LICENCIAMIENTO:

Todos los productos de Software que se utilicen deberán contar con factura y licencia de uso; por lo que se promoverá la regularización o eliminación de los productos que no cuenten con el debido licenciamiento.

El área de Sistemas promoverá y propiciará que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

4. ACCESO FÍSICO:

La clínica destinará un área que servirá como centro de telecomunicaciones donde ubicarán los sistemas de telecomunicaciones y servidores.

Todos los sistemas de comunicaciones estarán debidamente protegidos con la infraestructura apropiada de manera que el usuario no tenga acceso físico directo.

Entendiendo por sistema de comunicaciones: el equipo activo y los medios de comunicación.

El acceso de terceras personas debe ser identificado plenamente, controlado y vigilado durante el acceso.

Las visitas internas o externas podrán acceder a las áreas restringidas siempre y cuando se encuentren acompañadas cuando menos por un responsable del área de sistemas.

Las visitas a las instalaciones físicas de los centros de telecomunicaciones se harán en el horario establecido.

El personal autorizado para mover, cambiar o extraer equipo de cómputo es el área de sistemas, a través de formatos de autorización de Entrada/Salida, los cuales notificarán a las personas delegadas del área administrativa de la clínica y al personal de seguridad del edificio.

5. USO:

Los usuarios deberán cuidar, respetar y hacer un uso adecuado de los recursos de cómputo y de la red de la clínica, de acuerdo con las políticas que en este documento se mencionan.

Los usuarios deberán solicitar apoyo al área de sistemas ante cualquier duda en el manejo de los recursos de cómputo de la clínica.

El correo electrónico no se deberá usar para envío masivo, materiales de uso no institucional o innecesarios (entiéndase por correo masivo todo aquel que sea ajeno a la Las Empresas, tales como cadenas, publicidad y propaganda comercial, política, social, etcétera).

Se prohibirá el uso de dispositivos USB debido al alto riesgo de virus y filtración de información confidencial que estos representan, solo se permitirá el uso de estos a los usuarios autorizados por gerencia.

6. DERECHOS DE AUTOR:

Queda estrictamente prohibido inspeccionar, copiar y almacenar programas de cómputo, software y demás fuentes que violen la ley de derechos de autor.

Para asegurarse de no violar los derechos de autor, no está permitido a los usuarios copiar ningún programa instalado en los computadores de la clínica bajo ninguna circunstancia sin la autorización escrita de la Gerencia o del área de sistemas.

No está permitido instalar ningún programa en su computadora sin dicha autorización o la clara verificación de que la clínica de que posee una licencia que cubre dicha instalación.

No está autorizada la descarga de Internet de programas informáticos no autorizados por La Gerencia o el área de sistemas.

No se tolerará que un empleado realice copias no autorizadas de programas informáticos.

No se tolerará que un empleado cargue o descargue programas informáticos no autorizados de Internet, incluidos entre otros la descarga de programas informáticos para utilizar sistemas de peer-to-peer (P2P –Ej. Kazaa) que pueden utilizarse para comercializar trabajos protegidos por los derechos de autor.

No se tolerará un empleado realice intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.

Si se descubre que un empleado ha copiado programas informáticos o música en forma ilegal, este puede ser sancionado o amonestado según la decisión de gestión humana y el resultado del proceso disciplinario.

Si se descubre que un empleado ha copiado programas informáticos en forma ilegal para dárselos a un tercero, también puede ser sancionado o amonestado.

Si un usuario desea utilizar programas informáticos autorizados por las Empresas en su hogar, debe consultar con sistemas para asegurarse de que ese uso esté permitido por la licencia del editor.

El personal encargado de soporte de sistemas revisará las computadoras constantemente para realizar un inventario de las instalaciones de programas informáticos y determinar si la clínica posee licencias para cada una de las copias de los programas informáticos instalados.

Si se encuentran copias sin licencias, estas serán eliminadas y, de ser necesario, reemplazadas por copias con licencia.

Los usuarios utilizarán los programas informáticos sólo en virtud de los acuerdos de licencia y no instalarán copias no autorizadas de los programas informáticos comerciales.

Los usuarios no descargarán ni cargarán programas informáticos no autorizados a través de Internet.

Los usuarios no realizarán intercambios o descargas de archivos digitales de música (MP3, WAV, etc.) de los cuales no es el autor o bien no posee los derechos de distribución del mismo.

Los usuarios que se enteren de cualquier uso inadecuado que se haga en la clínica de los programas informáticos o la documentación vinculada a estos, deberán notificar al Gerente o director del área en la que trabajan o al asesor legal de la clínica.

Según las leyes vigentes de derechos de autor, las personas involucradas en la reproducción ilegal de programas informáticos pueden estar sujetas a sanciones civiles y penales, incluidas multas y prisión.

No se permite la duplicación ilegal de programas informáticos.

7. RED:

Las redes tienen como propósito principal servir en la transformación e intercambio de información dentro de la clínica entre usuarios, procesos, oficinas y hacia afuera a través de conexiones con otras redes.

El área de sistemas no es responsable por el contenido de datos ni por el tráfico que en ella circule, la responsabilidad recae directamente sobre el usuario que los genere o solicite.

Nadie puede ver, copiar, alterar o destruir la información que reside en los equipos sin el consentimiento explícito del responsable del equipo.

No se permite el uso de los servicios de la red cuando no cumplan con las labores propias de la clínica.

Las cuentas de ingreso a los sistemas y los recursos de cómputo son propiedad de la clínica y se usarán exclusivamente para actividades relacionadas con la labor asignada.

Todas las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles. Se permite su uso única y exclusivamente durante la vigencia de derechos del usuario.

El uso de analizadores de red es permitido única y exclusivamente por sistemas para monitorear la funcionalidad de las redes, contribuyendo a la consolidación del sistema de seguridad bajo las Políticas de Seguridad.

No se permitirá el uso de analizadores para monitorear o censar redes ajenas a la clínica y no se deberán realizar análisis de la

Red desde equipos externos a la entidad.

Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectará temporal o permanentemente al usuario o red involucrada dependiendo de las políticas. La reconexión se hará en cuanto se considere que el uso no aceptable se ha suspendido.

8. SEGURIDAD DE CÓMPUTO:

El área de sistemas es la encargada de suministrar medidas de seguridad adecuadas contra la intrusión o daños a la información almacenada en los sistemas así como la instalación de cualquier herramienta, dispositivo o software que refuerce la seguridad en cómputo. Sin embargo, debido a la

cantidad de usuarios, a la amplitud y constante innovación de los mecanismos de ataque no es posible garantizar una seguridad completa.

El área de sistemas debe mantener informados a los usuarios y poner a disposición de los mismos el software que refuerce la seguridad de los sistemas de cómputo.

El área de sistemas son los únicos autorizados para monitorear constantemente el tráfico de paquetes sobre la red, con el fin de detectar y solucionar anomalías, registrar usos indebidos o cualquier falla que provoque problemas en los servicios de la red.

9. FUNCIONES DE EL AREA DE SISTEMAS:

- Registrar cada máquina en el inventario de control de equipos de cómputo y red de la clínica.
- Auditar periódicamente y sin previo aviso los sistemas y los servicios de red, para verificar la existencia de archivos no autorizados, música, configuraciones no válidas o permisos extra que pongan en riesgo la seguridad de la información.
- Realizar la instalación o adaptación de sus sistemas de cómputo de acuerdo con los requerimientos en materia de seguridad.
- Reportar a la gerencia los incidentes de violación de seguridad, junto con cualquier experiencia o información que ayude a fortalecer la seguridad de los sistemas de cómputo.

10. USO APROPIADO DE LOS RECURSOS:

Los Recursos Informáticos, Datos, Software, Red y Sistemas de Comunicación están disponibles exclusivamente para complementar las obligaciones y propósito de la operativa para la que fueron diseñados e implantados. Todo el personal o usuario de dichos recursos debe saber que no tiene el derecho de confidencialidad en su uso.

Está prohibido:

- El uso de estos recursos para actividades no relacionadas con el propósito del negocio, o bien con la extralimitación en su uso.
- Las actividades, equipos o aplicaciones que no estén directamente especificados como parte del Software o de los Estándares de los Recursos Informáticos propios de la clínica.
- Introducir en los Sistemas de Información o la Red Corporativa contenidos obscenos, amenazadores, inmorales u ofensivos.
- Introducir voluntariamente programas, extensiones, virus, macros, applets, controles ActiveX o cualquier otro dispositivo lógico o secuencia de caracteres que causen o sean susceptibles de causar cualquier tipo de alteración o daño en los Recursos Informáticos.

- Intentar destruir, alterar, inutilizar o cualquier otra forma de dañar los datos, programas o documentos electrónicos.
- Albergar datos de carácter personal en las unidades locales de disco de los computadores de trabajo.
- Cualquier fichero introducido en la Red o en el puesto de trabajo del usuario a través de soportes automatizados, internet, correo electrónico o cualquier otro medio, deberá cumplir los requisitos establecidos en estas Políticas y, en especial, las referidas a propiedad intelectual y control de virus.

11. SEGURIDAD PERIMETRAL:

La seguridad perimetral es uno de los métodos de protección de la Red, basado en el establecimiento de recursos de seguridad en el perímetro externo de la red y a diferentes niveles.

Esto permite definir niveles de confianza, permitiendo el acceso de determinados usuarios internos o externos a determinados servicios, y denegando cualquier tipo de acceso a otros.

Sistemas de información implementará soluciones lógicas y físicas que garanticen la protección de la información de las compañías de posibles ataques internos o externos tales como:

- Rechazar conexiones a servicios comprometidos.
- Permitir sólo ciertos tipos de tráfico (p. ej. correo electrónico, http, https).
- Proporcionar un único punto de interconexión con el exterior.
- Redirigir el tráfico entrante a los sistemas adecuados dentro de la intranet (Red Interna).
- Ocultar sistemas o servicios vulnerables que no son fáciles de proteger desde internet.
- Auditar el tráfico entre el exterior y el interior.
- Ocultar información: nombres de sistemas, topología de la red, tipos de dispositivos de red cuentas de usuarios internos.

12. CONECTIVIDAD A INTERNET:

La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos los colaboradores de la clínica tienen las mismas responsabilidades en cuanto al uso de Internet.

El acceso a Internet se restringe exclusivamente a través de la Red establecida para ello, es decir, por medio del sistema de seguridad con Firewall incorporado en la misma.

No está permitido acceder a Internet llamando directamente a un proveedor de servicio de acceso y usando un navegador, o con otras herramientas de Internet conectándose con un módem.

Todas las actividades en Internet deben estar en relación con tareas y actividades del trabajo desempeñado.

Sólo puede haber transferencia de datos de o a Internet en conexión con actividades propias del trabajo desempeñado.

Está estrictamente prohibido el uso de programas para evitar las políticas de restricción de páginas web no institucionales, el uso de este tipo de software será sancionado o amonestado según decisión de gerencia y gestión humana.

Restricciones/prohibiciones de acceso a internet: Con la finalidad de hacer un buen uso de la red, se aplicarán las siguientes prohibiciones:

- El uso de programas para compartir archivos (Peer to Peer), o programas para evitar las políticas de restricción de navegación.
- El uso de programas para saltar proxis, firewalls y políticas de restricción.
- El acceso a páginas con cualquier tipo de contenido explícito de pornografía.
- El uso de sitios de videos en línea o en tiempo real.
- Debido a las limitaciones de ancho de banda existentes NO se permite la conexión a estaciones de radio por Internet.
- Uso de JUEGOS "on line" en la red.
- El ingreso a páginas web no institucionales o no afines a la labor que desempeña el personal.

13. EXCEPCIONES:

Entre las medidas de seguridad se encuentra configurado para restringir algunas palabras y sitios de Internet; por lo que pueden existir palabras o sitios que a pesar de ser inofensivos tendrán negado el acceso; en este caso, los usuarios podrán notificar esta eventualidad para que sea resuelta a la brevedad posible.

En caso de eventos, cursos, talleres, conferencias, etc, se podrán habilitar equipos con acceso a la red de manera temporal por el tiempo necesario previa solicitud de los interesados con una anticipación de por lo menos un día hábil y con la debida autorización del jefe inmediato.

14. ACCESO A INVITADOS (PROYECTO):

La red inalámbrica (W-GUEST) es un servicio que permite conectarse única y exclusivamente a personal externo de la clínica (clientes, proveedores, pacientes) a internet sin la necesidad de algún tipo de cableado. La Red inalámbrica de Invitados le permitirá utilizar los servicios de Internet, en las zonas de cobertura de la misma.

Los usuarios invitados no tendrán acceso a la Red de la clínica ni a ningún recurso de uso privado.

15. DISPOSICIONES:

Las disposiciones aquí enmarcadas, entrarán en vigor a partir del día de su difusión.

Las normas y políticas objeto de este documento podrán ser modificadas o adecuadas conforme a las necesidades que se vayan presentando, mediante acuerdo del Comité; una vez aprobadas dichas modificaciones o adecuaciones, se establecerá su vigencia.

La falta de conocimiento de las normas aquí descritas por parte de los usuarios no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.

16. CONTROL DE CAMBIOS:

Versión	Fecha	Descripción	Elaboró	Revisó	Aprobó
001	Noviembre 2015	Creación del documento	Grupo Sistemas de Información	Ivette Arce Coordinadora Calidad	Natasha Molina Gerente