CODIGO DE ETICA INFORMATICO DEL HOSPITAL JOSE ANTONIO SOCARRAS SANCHEZ

1. CÓDIGO DE ÉTICA INFORMÁTICA

El Presente documento reglamenta y amplía las políticas de uso de los sistemas de información definidas en el **"Manual de Políticas Corporativas del Hospital Jose Antonio Socarras Sanchez"** que contiene las líneas de conducta que sus empleados, consultores y contratistas deben observar para garantizar el continuo crecimiento personal, profesional y corporativo, en el marco del respeto por la institucionalidad y por las normas aplicables.

A continuación, encontrará las normas mínimas que debe conocer y cumplir en relación con el uso de los recursos informáticos (sistemas de información, computadores personales, servidores, impresoras, redes, software, correo electrónico e Internet, dispositivos móviles, entre otros) de la Empresa. Su incumplimiento podrá conllevar sanciones administrativas y/o las contempladas en la ley.

1.1 Generales

Utilizar los recursos informáticos con criterios de procedimientos y estándares establecidos y velar por su adopción en su área de influencia.

Desarrollar comportamientos seguros frente al uso de la tecnología.

Manejar la información con criterios de confidencialidad. Se deberá restringir el acceso general y cifrar los datos sensibles cuando sea requerido.

La información del Hospital no debe ser compartida, copiada, ni divulgada por ningún medio incluyendo el verbal sin las debidas autorizaciones de la alta gerencia.

Se deberá mantener la disponibilidad de la información de acuerdo con las normas legales y las necesidades del Hospital.

1.2 Control de acceso

Asignar palabras claves o contraseña de arranque, de set up (configuración), de protector de pantalla y los archivos confidenciales, entre otros recursos.

Los usuarios son responsables por las actividades realizadas bajo su nombre y contraseña asignada.

Reportar cualquier violación a las normas de control de acceso.

Las contraseñas o contraseña deben ser cambiados regularmente de acuerdo con las políticas de seguridad del Hospital, no deben almacenarse en sitios públicos y no pueden repetirse.

Si por efectos de mantenimientos o arreglos en las aplicaciones o computador de un usuario, éste debe compartir su contraseña con personal de IT u otro personal autorizado, la clave debe ser cambiada de manera inmediata una vez el proceso de soporte haya concluido.

No se deben intentar examinar, escanear o violar la seguridad de las medidas de autenticación de los sistemas o red.

1.3 Servicios

Solicitar formalmente los servicios informáticos que requiera, no se deberá acceder a sitios o servicios que no han sido autorizados expresamente.

Seguir, con criterios de eficiencia, el procedimiento establecido para el reporte de fallas e incidentes de seguridad.

Devolver a la Gerencia de Tecnología los recursos (hardware, software - disquetes, CD's, certificados de licenciamiento, documentación entre otros.) que ya no requiera.

No imprimir documentos innecesariamente. Revisar que los parámetros de impresión (tamaño del papel, impresora asignada, entre otros) sean adecuados.

Notificar al área de servicios de tecnología cuando:

- Sea, transferido o cambie su función, para actualizar sus datos y/o desactivar los servicios no requeridos.
- No va a hacer uso de los servicios por más de 20 días, cualquiera que sea el motivo (vacaciones, licencias y retiro, entre otras) para que sea desactivado temporalmente.
- No requiera alguno de los servicios autorizados.

El total de los archivos personales de los empleados incluyendo archivos de office, archivos de música, videos, fotografías, etc., no podrá sobrepasar en ninguno de los casos un 10% de la capacidad total del disco duro del computador que le sea asignado.

Los usuarios deberán crear una carpeta en su disco duro que identifique claramente que contiene archivos personales. Deben crearla en el directorio raíz del disco duro y bajo el nombre PERSONAL. (C: \PERSONAL) todos los archivos que estén almacenados en una ubicación diferente se darán como entendido como laborales y deben acatar las reglas descritas en ésta política.

No es permitido conectar a la red del Hospital computadores personales o de tercero sin previa autorización y verificación de las condiciones de seguridad, software y licenciamiento del software que tiene instalado. En caso de requerir conexión a la red de la compañía, se deberá contar con la autorización de la Gerencia de Tecnología, previo cumplimiento de las condiciones y estándares de seguridad de la compañía.

1.4 Correo electrónico interno

No utilizar el correo electrónico para:

- Permitir a otro usuario enviar mensajes utilizando su cuenta, sin aclarar el remitente.
- Propagar información confidencial la cual debe enviarse cifrada o entregarse en forma personal.
- Solicitar donativos, promover cadenas de mensajes de cualquier índole, promover obras de caridad, enviar mensajes políticos, religiosos, mensajes que puedan ser interpretados como difamatorios, intimidatorios u ofensivos.
- Avisos clasificados o boletines de cualquier índole sin la respectiva autorización de la Gerencia del área.
- El uso del correo para fines personales deberá ser racional.
- Discutir temas para los cuales sea más efectivo utilizar otro medio, como el

teléfono, personalmente o convocar a una reunión.

- Enviar indiscriminadamente, a grandes grupos de usuarios, mensajes que puedan congestionar la red (con gráficos, imágenes, etc.).

Verificar que los archivos que se adjunten a los mensajes no contengan virus.

Evitar enviar anexos pesados, tales como fotos, que pueden bajar la velocidad del sistema y perjudicar su uso.

Responder por el contenido de los mensajes enviados y no alterar los recibidos sin la autorización del emisor.

Los mensajes enviados a nivel corporativo deberán ser canalizados a través de la Jefatura de Comunicaciones o en su defecto de la Gerencia autorizada para este tipo de comunicados.

No se debe acceder al buzón de entrada de otra persona u otras carpetas de correo electrónico, ni enviar correo electrónico que aparente venir de otra persona sin autorización explícita de esa persona, por ejemplo, a través de los delegados de Outlook.

Se acepta que los usuarios ocasionalmente puedan utilizar los servicios de tecnología y el correo electrónico para propósitos personales. bajo la condición de que todos los procedimientos y reglas establecidos en esta política sean cumplidos. Los usuarios deben ser conscientes, sin embargo, que, si ellos escogen hacer uso de estos dispositivos para correspondencia personal, la privacidad es limitada debido a que el Hospital puede necesitar monitorear las comunicaciones.

1.5 Internet: Navegación y Correo

Utilizar mensajería instantánea para actividades relacionadas con la gestión de negocio, y que estén expresamente autorizadas por la la Gerencia. La transmisión de archivos por este medio deberá ser restringida.

Responder por el uso de Internet (correo, grupos de discusión, etc.) ante terceros, eximiendo a la Empresa de cualquier responsabilidad derivada del uso indebido de estos recursos.

El uso de este servicio para fines personales deberá ser racional.

No permitir a otra persona enviar correos utilizando su cuenta sin aclarar el remitente.

El uso de Internet para la adquisición y contratación de bienes y servicios para el Hospital deberá seguir y/o ajustarse la normatividad definida, en este tema.

Cualquier adquisición de bienes y servicios que un usuario haga, vía Internet y a título personal, desde la infraestructura informática y de telecomunicaciones del Hospital, correrá por cuenta y riesgo de este y eximirá a la empresa de cualquier responsabilidad.

No se deberá utilizar para funciones del Hospital, software adquirido a través de Internet. Sólo la Gerencia de tecnología está autorizada para esto.

No use los sistemas del Hospital para bajar o distribuir software, canciones, vídeos u otros datos protegidos por derechos de autor.

1.6 Software

Utilizar solamente software legalmente adquirido. En caso de presentarse algún tipo de reclamación, ésta recaerá sobre el usuario responsable del activo en el que se encontrase dicho software. El usuario del software no deberá:

- Copiar, vender, regalar, distribuir o enajenar el software o su documentación sin permiso del autor.
- Estimular, permitir, obligar o presionar a los empleados a crear o utilizar copias no autorizadas.
- Alterar, modificar o adaptar el software y la documentación, incluyendo, entre otras acciones, la traducción, ingeniería reversa del código, desensamblado o creación de trabajos derivados.
- Utilizar hardware o software de monitoreo de actividades (analizadores de protocolos, software catalogado como "hacking", etc.) sin la debida autorización.

Aplicar las siguientes medidas preventivas para disminuir los riesgos de contagio de virus informáticos:

- No usar software ilegal o no licenciado.
- Mantener activa en el equipo la última versión del antivirus autorizada para la empresa y efectuar periódicamente revisiones al disco duro.
- Utilizar el software de detección de virus antes de leer un disquete, CD, DVD o memoria USB y antes de utilizar un nuevo software.
- Desconectarse de la red antes de probar software sospechoso (información bajada de Internet, software en demostración, software de libre distribución, entre otros).
- Verificar la confiabilidad de la fuente de origen de la información que se baja de Internet, antes de efectuar la operación. Por ejemplo: Sitios reconocidos como IBM o Microsoft tienen menos probabilidad de que contengan virus.
- Ejecutar un programa en dos o más computadores simultáneamente, a no ser, que esté específicamente permitido en la licencia.
- Infringir las leyes sobre copias no autorizadas, por orden de funcionarios con jerarquía de dirección en la empresa, o grupos de apoyo que lo soliciten.
- Prestar los programas para que sean copiados, o copiar los programas que han sido pedidos en préstamo.

ORIGINAL FIRMADO
DAIRIS ARMENTA
GERENTE

2. DECLARACIÓN - CÓDIGO DE ÉTICA INFORMÁTICA

Por medio de la presente, manifiesto que leí y entendí las disposiciones y condiciones estipuladas en este código de ética informática en el uso seguro y eficiente de los recursos tecnológicos del Hospital JOSE ANTONIO SOCARRAS SANCHEZ y acepto la aplicación de sus términos y me comprometo a seguir los procedimientos detallados en este documento. De igual manera me comprometo a conocer y a cumplir cualquier otra Norma y Directriz que en materia de Tecnología Informática y de Comunicaciones establezca el Hospital.

Declaro que entiendo totalmente que cualquier violación o no seguimiento de estas normas pueden acarrear una acción disciplinaria o legal, que pueden resultar en mi despido del Hospital.

Nombre: _____

Firma: _____

Registro / Identificación: _____ Fecha: _____