Tabla de contenido

Generales

Alcance

Esta política es aplicable a todos los empleados, contratistas, otros servidores de la empresa, incluyendo al personal externo que cuente con equipos conectados a la red de datos de la entidad.

Objetivo

Dotar de información necesaria a los usuarios, empleado de las normas y de los mecanismos que deben cumplir y utilizar para proteger el hardware y software de la entidad, así como los datos que son capturadas, procesados, almacenados y distribuidos en la entidad.
Planear, organizar, dirigir y controlar las actividades para mantener y garantizar los recursos informáticos, así como resguardar los activos de la entidad.

Vigencia

La documentación presentada como Políticas de Seguridad entrara en vigencia desde el momento en que sean aprobadas por la Gerencia. Esta normatividad deberá ser revisada y actualizada conforme a las necesidades de la entidad, o en el momento en el que se realicen cambios sustanciales en la infraestructura.

Notificaciones de violaciones de seguridad

Es de carácter obligatorio para el personal de la entidad la notificación de algún problema o violación de la seguridad, de la cual fuere testigo, esta notificación debe hacer por escrito vía correo electrónico.

Definiciones

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.
Backup: Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.
Contraseña: Clave de acceso a un recurso informático.
Control: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, etc. que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
Directrices: Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.
Servicios de procesamiento de la información: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.

Seguridad de la Información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas.
Evento de seguridad de la información: Es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.
Firewall: Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.
Incidente de seguridad de la información: Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones de la Cámara de Comercio y amenazar la seguridad de la información.
LAN: Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio ó una oficina).
Licencia de Software: Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación
Copyright: Son el conjunto de derechos de exclusividad con que la ley regula el uso de una particular expresión, de una idea o información. En términos más generalizados se refiere a los derechos de copia de una obra (poemas, juegos, trabajos literarios, películas, composiciones musicales, grabaciones de audio, pintura, escultura, fotografía, software, radio, televisión, y otras formas de expresión de una idea o concepto), sin importar el medio de soporte utilizado (Impreso, Digital), en muchos de los casos la protección involucra un periodo de duración en el tiempo. En muchos casos el copyright hace referencia directa a la protección de los derechos patrimoniales de una obra.
Propiedad Intelectual: Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.
Open Source: El **código abierto** es un modelo de desarrollo de software basado en la colaboración abierta
Software Libre: Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.
Software pirata: Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.
Software de Dominio Público: Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.
Freeware: Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado
Shareware: Clase de software o programa, cuyo propósito es evaluar por un determinado tiempo, o con unas funciones básicas permitidas. Para adquirir el software de manera completa es necesario un pago económico
Monitoreo: Verificación de las actividades de un usuario con respecto a los recursos informáticos de la Cámara de Comercio.
Plan de contingencia: Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de la Cámara de Comercio en casos de desastres y otros casos que impidan

el funcionamiento normal.
Política: Toda intención y directriz expresada formalmente por la dirección.
Protector de pantalla: Programa que se activa a voluntad del usuario, ó automáticamente después de un tiempo en el que no ha habido actividad.
Proxy: Servidor que actúa como puerta de entrada a la Red Internet.
Recursos informáticos: Elementos de tecnología de Información tales como: computadores servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, programas y datos.
Riesgo: Combinación de la probabilidad de un evento y sus consecuencias.
Análisis de Riesgos: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
Evaluación de Riesgos: Todo proceso de análisis y valoración del riesgo.
Valoración del Riesgo: Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.
Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
Router: Equipo que permite la comunicación entre dos o más redes de computadores.
Sesión: Conexión establecida por un usuario con un Sistema de Información.
Sistema de control de acceso: Elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas
Sistema de detección de intrusos (IDS): Es un conjunto de hardware y software que ayuda en la detección de accesos ó intentos de acceso no autorizados a los recursos informáticos de la Cámara de Comercio.
Sistema operativo: Software que controla los recursos físicos de un computador.
Usuario: Toda persona que pueda tener acceso a un recurso informático de la Cámara de Comercio.
Usuarios de red y correo: Usuarios a los cuales la entidad les entrega un identificador de cliente para acceso a sus recursos informáticos.
Usuarios externos: Son aquellos clientes externos que utilizan los recursos informáticos de la entidad a través de Internet ó de otros medios y tienen acceso únicamente a información clasificada como pública.

Políticas Generales de Seguridad Informática

Políticas de cumplimiento y sanciones

Cumplimiento con la seguridad de la información

Todos los funcionarios de la entidad, así como los contratistas, deben cumplir y acatar las políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por su estricto cumplimiento a la gerencia y Oficial de Seguridad de la Información.

Medidas disciplinarias por incumplimiento de políticas de seguridad

Todoincumplimientodeunapolíticadeseguridaddelainformaciónporpartedeunfuncionarioocontratista,asícomo de cualquier estándar o procedimiento es causa para iniciar acciones disciplinarias.

Políticas de uso de recursos informáticos

Instrucciones para el uso de recursos informáticos

El uso de cualquier sistema de información y demás recursos informáticos por parte del empleado, trabajadores o usuarios de los sistemas de La Corporación Hospital Infantil Concejo de Medellín, debe someterse a todas las instrucciones técnicas, que

imparta la entidad.

Uso personal de los recursos

Los recursos informáticos de La Corporación Hospital Infantil Concejo de Medellín, dispuestos para la operación, solo deben ser usados para fines laborales. El producto del uso de dichos recursos tecnológicos será de propiedad de la Entidad.

Acuerdo de confidencialidad

Para el uso de los recursos tecnológicos de La Corporación Hospital Infantil Concejo de Medellín, todo usuario debe firmar un acuerdo de confidencialidad antes de que le sea otorgado su Login de acceso a la red y sus respectivos privilegios o medios de instalación.

Prohibición de instalación de software y hardware en los computadores de La Corporación Hospital Infantil Concejo de Medellín.

La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos solo puede ser realizada por los funcionarios de sistemas autorizados por el Hospital.

Uso del aplicativo entregado.

La Corporación Hospital Concejo de Medellín contrata con las empresas desarrolladores de software y proveedores "LICENCIA DE USO" para los aplicativos que utiliza. Está terminantemente prohibido copiar cualquiera de los aplicativos que se aloja en los computadores de La Corporación Hospital Infantil Concejo de Medellín, esto se asegura con la firma del Acuerdo de Confidencialidad para los usuarios y con la firma del contrato realizado con los proveedores que maneje información de la entidad, adicional a esto cada usuario, dependiendo de las actividades que realice sobre las aplicaciones maneja un rol limitado, de esta forma es controlado el acceso.

El usuario es responsable por toda actividad que involucre su identificación personal(Usuario) o recursos informáticos asignados.

Todo usuario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien esta le fue otorgada. Los usuarios no deben permitir que ninguna otra persona realice labores bajo su identidad. De forma similar, los usuarios no deben realizar actividades bajo la identidad de alguien más. La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del usuario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a sistemas de la entidad.

Declaración de reserva de derechos de La Corporación Hospital Infantil Concejo de Medellín

El Hospital usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada por sistemas de información. Para mantener estos objetivos la entidad se reserva el derecho y la autoridad de:

- Restringir o revocar los privilegios de cualquier usuario
- Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados
- Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de la entidad.

Esta autoridad se puede ejercer con o sin conocimiento de los usuarios, bajo la responsabilidad del Director de TI de la entidad.

Recursos compartidos.

Cuando exista la necesidad de compartir recursos esto se debe hacer con autorización del Director de TI de la entidad.

Acceso no autorizado a los sistemas de información de la Entidad

Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios y de alguna forma dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de inscripción y otros mecanismos de control de acceso que le puedan permitir obtener ingreso a sistemas no autorizados.

Posibilidad de acceso no implica permiso de uso

Los usuarios no deben leer, modificar, copiar o borrar información perteneciente a otro usuario sin la debida autorización de este

Prohibición a la explotación de vulnerabilidades de seguridad de los recursos informáticos

A no ser que exista una aprobación por escrito para ello o sea parte de su función laboral, los usuarios no deben explotar las deficiencias de seguridad de los sistemas de información para dañar los sistemas o la información contenida en ellos, obtener acceso a recursos a los cuales no se le ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato al Líder de TI de la entidad.

Manejo de sesiones en sistemas informáticos

Si el usuario está conectado a un sistema que contiene información sensible, éste no debe dejar el computador desatendido sin cerrar primero la sesión iniciada.

Notificación de sospecha de pérdida, divulgación ó uso indebido de información

Cualquier incidente de Seguridad debe reportarse por escrito al correo electrónico del Líder de Ti de la Entidad.

Traslado de equipos debe estar autorizado

Ningún equipo de cómputo debe ser reubicado o trasladado dentro o fuera de las instalaciones del hospital sin previa autorización. Así mismo, ningún equipo de cómputo debe ser reubicado o trasladado de las instalaciones de la entidad a la que fue asignado. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal de sistemas autorizado

Control de recursos informáticos entregados a los usuarios

Cuando un usuario inicie su relación laboral con la entidad se debe diligenciar el documento de entrega de inventario. Cuando un empleado termine su vinculación laboral con la Entidad, sea trasladado a otra oficina o por alguna otra circunstancia deje de utilizar el computador personal o el recurso tecnológico suministrado con carácter permanente, deberá hacerse una validación de lo entregado por el usuario contra lo registrado en el formato de descargue de inventario. El empleado será responsable de los deterioros o daños que por su negligencia haya ocasionado a los equipos de hardware.

Configuración de sistema operativo de las estaciones de trabajo

Solamente los funcionarios del área técnica de sistemas están autorizados para cambiar la configuración del sistema operativo de las estaciones de trabajo de los usuarios

Custodia de Licencias de Software

Las licencias deben ser custodiadas y controladas por el área de Sistemas. Esta área debe realizar

auditorías de licencia de software como mínimo una vez al año generando las evidencias respectivas, lo anterior para garantizar que los funcionarios solo tienen instalado software legal y autorizado por la entidad.

Apagado de equipos en lanoche

Con fin de proteger la seguridad y distribuir bien los recursos de la empresa, los equipos de cómputo deben quedar apagados cada vez que no haya presencia de funcionarios en la oficina, disminuyendo los consumos de energía y alargando la vida útil del equipo.

Lineamientos para la adquisición de bienes informáticos.

Del Hardware

La adquisición de tecnología informática (ATI) se efectuará a través del comité de compras. Los ATI, al planear las operaciones relativas a la adquisición de bienes informáticos, establecerán prioridades y en su selección deberá tomarse en cuenta:
Precio: Costo inicial, costo de mantenimiento y consumibles por el periodo estimado de uso.
Calidad: Características técnicas de los recursos informáticos.
Experiencia: Estructura de servicio, certificados de calidad.
Estándares: La arquitectura se basa en los estándares, y debe tener una permanencia mínima de dos a cinco años.
Capacidades:

- El equipo debe estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores de este.
- Cumplir con los últimos estándares de la industria
- Garantía mínima de 5 año para los equipos con soporte en el sitio (Estaciones, Portátiles, Servidores)
- Garantía mínima de 6 meses en impresoras, Scaner, Switches, etc
- Los equipos deben ser de marcas reconocidas a nivel del medio (HP, Dell, Lenovo), contar con presencia y permanencia demostrada en el mercado nacional, así como asistencia técnica y de repuestos local.

Del Software

Los productos de software que se adquieren cumplen con los requisitos y requerimientos específicos de la institución, en cuanto a la plataforma de software y de hardware. Tienen una alta calidad en cuanto al grado que satisface los requerimientos de la institución: precisión requerida, cantidad de recursos utilizados, control del acceso, facilidad de uso, facilidad de mantenimiento y prueba, portabilidad del software y facilidad de ínter operación. Todos los aplicativos trabajan en ambiente WEB.
Todo el software de la empresa está licenciado respetando los derechos de autor y se mantiene actualizado permanentemente con los parches y mejoras que le realizan al software.
Las licencias que se adquieren son las últimas que existen en el mercado y están probadas.
Se vela por las actualizaciones periódicas de los programas antivirus, sistemas operativos, software de

oficina, manejador de bases de datos, utilitario etc.
En cuanto a la paquetería sin costo se respeta la propiedad intelectual intrínseca del autor.
La oficina de sistemas promueve y propicia que la adquisición de software de dominio público provenga de sitios oficiales y seguros.

Del software propiedad de la institución.

Toda la programática adquirida por la institución sea por compra, donación o cesión es propiedad de la institución y mantiene los derechos que la ley de propiedad intelectual le confiere.
La oficina de sistemas tiene un registro de todos los paquetes de programación propiedad del HOSPITAL.
Todos los sistemas programáticos (programas, bases de datos, sistemas operativos, interfaces) desarrollados con o a través de los recursos del HOSPITAL se mantienen como propiedad de la institución respetando la propiedad intelectual del mismo.
Es obligación de todos los usuarios que manejen información masiva, mantener el respaldo correspondiente de la misma ya que se considera como un activo de la institución que debe preservarse.
Los datos, las bases de datos, la información generada por el personal y los recursos informáticos de la institución están resguardados.

De la propiedad intelectual.

La oficina de sistemas procura que todo el software instalado en el hospital esté de acuerdo con la ley de propiedad intelectual a que dé lugar, cumpliendo con las políticas de derechos de autor, por tanto, el software que se utilice deberá contar con su factura y licencia de uso respectiva.

De las bases de datos.

El acceso al sistema de información deberá contar con los privilegios o niveles de seguridad de acceso suficientes para garantizar la seguridad de la información de la empresa. Los niveles de seguridad de acceso deben controlarse con un sistema de parametrización.

- Se debe delimitar los permisos de consulta, edición, modificación, eliminación.
- Las bases de datos deben ser respaldadas, según plan de copias de seguridad.
- Las bases de datos deben contar con un log de transacciones que permite monitorizar la trazabilidad de los datos.
- Frecuencia de evaluación de las políticas
- Se evaluarán las políticas presentes en este documento, con una frecuencia anual.

Políticas de seguridad Física

Del acceso a áreas críticas

El acceso al área de Informática está restringido:
• Sólo ingresa al área el personal que trabaja en la misma.
• El ingreso de personas externo solo podrá ser bajo una autorización del Líder de Ti de la entidad.
• Siempre esta área debe permanecer cerrada, limpia y organizada.
• Las visitas al área de Informática o centro de cómputo por personas ajenas a la entidad, podrán hacerlo con previa identificación personal y sólo para realizar labores propias del área.
• Esta área debe recibir aseo y mantenimiento por lo menos una vez al día y sus adecuaciones físicas se realizan de acuerdo con las normas de seguridad establecidas para tal fin.

Del control de acceso al equipo de cómputo.

Cualquier Terminal que pueda ser utilizada como acceso a los datos de un Sistema controlado, es encerrada en un área segura o guardada, de tal manera que no sean usadas, excepto por aquellos que tengan autorización para ello.
Restricciones que se aplican:

- Determinación de los períodos de tiempo para los usuarios a las terminales.
- Designación del usuario por la Terminal o de la Terminal por usuario.
- Limitación del uso de programas para usuario o terminales.
- Límite de tentativas para la verificación del usuario.
- Tiempo de validez de las contraseñas.

Dada la naturaleza insegura de los sistemas operativos y su conectividad en la red, la oficina de sistemas tiene la facultad de acceder a cualquier equipo de cómputo del hospital.
En los lugares donde se tienen instalados los equipos informáticos está prohibido consumir alimentos.

Del control de acceso local a la red.

Los programas de control de acceso identifican los usuarios autorizados a usar determinados sistemas, con su correspondiente nivel de acceso. Las distinciones que existen en los niveles de acceso están referidas a la lectura o modificación en sus diferentes roles
La oficina de sistemas es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.
Dado el carácter unipersonal del acceso a la red, la oficina de sistemas verifica el uso responsable de las tecnologías de la información.
El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, etc.) conectado a la red es administrado por la oficina de sistemas.
Todo el equipo de cómputo que esté o sea conectado a la Red o aquellas que en forma autónoma se tengan y que sean propiedad de la institución, debe sujetarse a los procedimientos de acceso que emite la oficina de sistemas.

De acceso a los sistemas administrativos.

La instalación y uso de los sistemas de información se rigen por las políticas de la oficina de sistemas:
A los servidores de bases de datos administrativos, se prohíbe el acceso de cualquier usuario, excepto para el personal del departamento de Informática.
El control de acceso a cada sistema de información de la entidad es determinado por la oficina de sistemas quien es responsable de asignar los perfiles de los usuarios y definir los grupos de trabajo.

De acceso a la información.

Todas las personas que laboran en el hospital o terceros autorizados para acceder a la red corporativa deben identificarse mediante la utilización de códigos de usuario, claves de acceso. Los códigos de usuarios son asignados por la oficina de sistemas, previa autorización escrita del coordinador de área, informando en que módulos va a trabajar y cuáles son las funciones asignadas.
Las solicitudes de códigos de usuarios son realizadas a la oficina de sistemas, certificando su capacitación, indicando el perfil, previa autorización del coordinador del área.
La clave de acceso a la red tiene fecha de expiración y el usuario está obligado a modificarla. Si después de tres (3) solicitudes de cambio no lo realiza, el sistema rechazará todo intento de ingreso, y solo podrá reactivarse el usuario comunicándose con los administradores del sistema.

Cuando un usuario se retira del hospital o es trasladado a otro servicio es deber del coordinador del servicio solicitar oportunamente el retiro o cambio de permisos a la oficina de sistemas.

De la instalación de equipo de cómputo.

Todo el equipo de cómputo (computadoras, estaciones de trabajo, servidores y equipos periféricos), que esté o sean conectado en la institución o aquel que en forma autónoma se tenga y que sea propiedad de la institución debe cumplir con los siguientes requisitos:

- Visto bueno por el área de sistemas
- Estar cubierto por el seguro contra corriente débil
- Estar etiquetado y relacionado en el inventario del área a la cual se ha asignado.
- Contar con una adecuada instalación eléctrica
- Verificar que el área de trabajo sea segura y cuente con el inmobiliario mínimo para su uso.
- Los equipos informáticos no deben instalarse cerca de ventanales en los cuales entra directamente la luz del sol, ya que el calor puede dañar los circuitos electrónicos.
- La oficina de sistemas tiene un registro de todos los equipos propiedad del hospital.
- El equipo de la institución que sea de propósito específico y tenga una misión crítica asignada, será ubicado en un área que cumpla con los requerimientos de: Seguridad física, las condiciones ambientales, la alimentación eléctrica.
- La protección física de los equipos corresponde a quienes en un principio se le asigna, y corresponde notificar los movimientos en caso de que existan, a la oficina de sistemas.
- Todo equipo que se conecte a la red de datos de la empresa debe tener instalado programa de antivirus debidamente licenciado y actualizado. El programa debe residir en memoria y monitorizado por la consola de administración del antivirus.
- La instalación de equipos de cómputo del hospital debe ser autorizado y realizado por personal de la oficina de sistemas.
- La capacitación al usuario debe ser realizado por el líder de la aplicación o por el funcionario que éste delegue.
- La inducción sobre el manejo específico de los recursos informáticos que el hospital entregue al usuario final está a cargo de la oficina de sistemas.
- Todas las personas que requieran del sistema de información para el desempeño de sus funciones deben previamente acreditar conocimientos básicos del sistema operativo WINDOWS, y del software de oficina OFFICE, y en lo posible certificados por instituciones reconocidas en el medio.

Políticas de seguridad lógica

Red

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

Nadie puede ver, copiar 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 cuando no cumplan con las labores propias de la entidad.
Las cuentas de acceso a los sistemas y recursos de las tecnologías de información son personales e intransferibles.
El uso de analizadores de red es permitido única y exclusivamente por el personal del área de TI.
Cuando se detecte un uso no aceptable, se cancelará la cuenta o se desconectara temporalmente al usuario o red involucrada.

Servidores

El área de TI es la responsable de la instalación, configuración e implementación de la seguridad, de los servidores conectados en la red.
Los servidores deben recibir mantenimiento mínimo dos veces al año.
Ser monitoreados por el área de TI. (Discos, memoria, procesadores, ventiladores, tarjetas de red, accesos, logs)
La información de los servidores deberá ser respaldada diariamente.

Del Correo electrónico.

El área de TI se encargará de asignar las cuentas de correo.
Para la asignación de un correo electrónico empresarial debe enviar la solicitud al correo de sistemas.
La longitud mínima de la contraseña será de 8 caracteres.
No hay correos de destinatarios desconocidos y/o que no hacen referencia al asunto.
No está permitido reenviar correos basuras o SPAM.
Se usa el correo a través de la página de mail.corporacionhicm.org.

De las Bases de datos

El área de TI no deberá eliminar ninguna información del sistema.
El área de TI es la encargada de asignar las cuentas a los usuarios.
La contraseña será asignada por el área de TI, la cual debe contener como mínimo 10 caracteres, incluir mayúsculas y minúsculas, número y caracteres especiales.

Recursos de computo

El área de TI debe poner a disposición de los usuarios el software que refuerce la seguridad del sistema de cómputo.
El área de TI es la única autorizada para monitorear constantemente el trafico 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.

Soporte Técnico

Podrán ingresar en forma remota única y exclusivamente para la solución de problemas.
Deberá actualizar el inventario de los equipos
Deberá auditar los servicios de red y los sistemas para verificar la existencia de archivo no autorizados.
Reportar los incidentes de violaciones de seguridad.

Renovación de equipos

Se deben definir los tiempos estimados de vida útil de los equipos de cómputo.
Por necesidades del servicio se puede solicitar el cambio del equipo, el cual será verificado y autorizado por el área de TI.

Usuarios

Del manejo de las contraseñas

- Evite utilizar contraseñas que tengan palabras que se pueden encontrar en el diccionario, ya que son más fáciles de violar mediante el uso de software especializado.
- Evite el uso de información que lo defina y que sea fácil de encontrar, como los números de su teléfono o los nombres de personas allegadas etc.
- Evite utilizar la misma contraseña.
- Cambie sus contraseñas con frecuencia.
- Utilice claves que son mezclas aleatorias de números y letras. Si es posible, también mezcle caracteres en mayúsculas y minúsculas.
- No revele su contraseña. De nada sirve crear una palabra clave que no se pueda violar, si la deja apuntada en un papel pegado a su computador.
- La contraseña debe contener como mínimo 8 caracteres.
- La contraseña se inactivará después de tres intentos fallidos.

Antivirus

- Todos los equipos deben contar con un antivirus instalado y actualizado.
- Las estaciones de trabajo deben ser monitorizadas desde la consola de administración instalada en el servidor.
- La estación de red se aislará si se detecta un virus que pueda afectar la seguridad de la red.

Seguridad Perimetral

Permite establecer recursos de seguridad en el perímetro externo de la red a diferentes niveles, definiendo niveles de confianza y permitiendo el acceso a determinados usuarios a determinados servicios y denegando cualquier otro tipo de servicio.

Gestor Unificado de Amenazas

Detecta accesos no autorizados.
Se encarga de controlar puertos y conexiones.
Permite establecer reglas necesarias para bloquear, permitir o ignorar el flujo de datos entrante y saliente.
Permite establecer el número de conexiones permitidas y bloquear cuando supera estas.
Controlas las aplicaciones y paginas autorizadas.

Redes Privadas Virtuales

El área de TI configurar el software necesario y asignara las claves a los usuarios.

De la actualización del software.

El área de TI realiza la actualización de software.

Las actualizaciones del software de uso común o más generalizado se llevan a cabo en línea y para ello se destinan unos puntos de actualización a los cuales los usuarios pueden tener acceso.

Acceso a internet

El acceso a internet se concede exclusivamente para actividades del trabajo.
Está prohibido usar servicios proxy para acceder a internet.
El hospital define a que usuarios les autoriza el acceso a Internet.
El acceso a Internet es autorizado por la oficina de sistemas, acorde a políticas institucionales.
El hospital restringe a los usuarios a descargar archivos que pongan en riesgo la seguridad de la red de datos y el desempeño del canal de comunicaciones con Internet. Estos archivos son música (*.mp3), Videos (*.MPG, *.avi), *.EXE, .COM, .DAT, .PIF, etc.

De la Página Web

La página Web es actualizada periódicamente como mínimo una vez al mes.
Los archivos que se publican son en formato PDF, protegidos contra cambios.