PLAN ESTRATEGICO DE SISTEMAS

POLITICAS, ESTANDARES EN SEGURIDAD INFORMATICA DE LAS TIC

HOSPITAL DEPARTAMENTAL SAN RAFAEL ZARZAL

2016-2017

ADMINISTRACIÒN DE CUENTAS DE USUARIO

ADMINISTRACIÓN Y USO DE CONTRASEÑAS

- ✓ Para la creación de las contraseñas en el sistema la política es que cada contraseña se cree el usuario con la primera letra del nombre, seguido del primer apellido, y la contraseña asignada son los 4 últimos números de la cedula, la cual debe ser cambiada por el usuario en el mismo momento en que este entre al sistema sihos.

- ✓ La asignación de contraseñas debe ser realizada de forma individual lo que el uso de contraseñas compartidas está prohibido,

- ✓ Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá acudir al área de sistemas para que se le proporcione una nueva contraseña o en su defecto usted podrá cambiarla por el mismo aplicativo.

- ✓ Está prohibido que las contraseñas se encuentren de forma legible en cualquier medio impreso y dejarlos en un lugar donde personas no autorizadas puedan descubrirlos.

- ✓ Sin importar las circunstancias, las contraseñas nunca se deben compartir o revelar.

- ✓ Hacer esto responsabiliza al usuario que prestó su contraseña de todas las acciones que se realicen con el mismo.

- ✓ Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, deberá cambiarlo inmediatamente.

- ✓ Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

RESPONSABLE: Ingeniero de sistemas

PROCEDIMIENTO PARA LA ACTUALIZACION DEL SITIO WEB CON BASE GOBIERNO EN LINEA (TIC)YLA PARTICIPACION EN LA RED SOCIAL FACEBOOK

Desarrollo del Sitio web:

EL ingeniero de sistemas del Hospital desarrolla, actualiza e implementa el sitio web, el cual es alimentado con la información de todas las áreas de servicio del hospital tanto financiera como asistencial.

La empresa en donde se tiene

Procedimiento:
Cada jefe de área y la gerencia envían la información pertinente a lo que se requiere subir teniendo en cuenta comitec tic y normatividad de ley del **Ministerio de las TIC** y bajo los lineamientos de **Gobierno En Línea**, regidos por las siguientes reglamentos.

Decreto1151 abril 14 de2008: Por el cual se establecen los lineamientos generales de la estrategia del gobierno en Línea de la Republica de Colombia, se reglamenta parcialmente la ley 962 de 2005 y se dictan otras disposiciones.

Ley 1712 del 6 de marzo de 2014:"por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones".

DECRETO 2693 de 2012- gobierno en líneaETAPAS Y COMPONENTES DE LA POLÍTICA ANTITRÁMITES Y DE GOBIERNO EN LÍNEA

El dominio registrado para entrar al sitio web es: www.hospitalsanrafaelzarzal.gov.co
Facebook y la

Lo que se publica como noticia principal en el sitio web, es lo que se sube al Facebook del hospital el oficial para mantener actualizado a otro tipos de usuarios, correo electrónico como lo encuentran es facebook@hospitalsanrafaelzarzal.gov.co

RESPONSABLE DEL DESARROLLO, ACTUALIZACION, IMPLEMENTACION DE LOS SITIOS DEL HOSPITAL ES: Ingeniero de Sistemas

1. **PROCEDIMIENTO PARA LA ADMINISTRACION DE CUENTAS DE USUARIO:**

Para acceder al sistema sihos debe pasar por la agremiación o si es rural por la oficina de personal en donde es allí donde definen al área de sistemas que usuario se creara en el sistema sihos, luego se le da un usuario y una contraseña para y si es médico o asistencial debe entregar al área de sistemas la firma con el sello para subirlo al sistema.

Cada novedad de los usuarios del sistema como vacaciones, permisos, licencias, retiros etc, debe ser reportada por la agremiación o por la oficina de personal por escrito o por correo electrónico, con el fin de realizarse el cambio respectivo.

RESPONSABLE: Ingeniero de sistemas

2. **LAS CUENTAS DE USUARIO Y SU APROBACION:**

Se solicita por correo electrónico la oficina de agremiación y talento humano verifica que si se realice la modificación y su inactivación si es el caso.

- ✓ **RESPONSABLE DE LOS DATOS INTERNOS**: Ingeniero de Sistemas revisa periódicamente las cuentas y verifica los retiros y las actualizaciones del sistema que no tengan inconvenientes los usuarios.
- ✓ **RESPONSABLE DEL SISTEMA SIHOS**:Empresa Sinergia encargado del soporte y actualización de la información.

LICENCIAMIENTO DE SOFTWARE

Como política de seguridad se tiene establecido en el Reglamento de Uso de las areas funcionales, la prohibición de instalar software y programas no autorizados y sin licencia. El área de sistemas realiza trimestralmente el mantenimiento preventivo un inventario físico de los programas y software instalados en cada uno de los computadores de la Institución.

3. **MODIFICACION DEL SISTEMA**

RESPONSABLE DEL CIERRE DE HISTORIAS CLINICAS: los médicos del hospital, son los encargados del cierre y su verificación.

RESPONSABLE DE ABRIR HISTORIAS CLINICAS: Las jefes de enfermeras y la ingeniera de sistemas, con el nombre de la admisión y una descripción que informe por qué se va abrir.
RESPONSABLE: Ingeniero de sistemas, jefes de enfermeras

4. ADMINISTRACIÓN DE PRIVILEGIOS

- ✓ Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados al área de sistemas (Administrador de la Red), para el cambio de privilegios.
- ✓ **RESPONSABLE:** Ingeniero de sistemas

- ✓ **RESPONSABLE DEL MANTENIMIENTO DE LA BASE DE DATOS:**El ingeniero de sistemas cogela carpeta cron ubicada en el servidor central donde está instalado el sistema sihos, que no se encuentre llena y que mensualmente se esté borrando las copias repetidas y solo se deje una por mensual hasta tener por año 12 que luego son almacenadas en un disco duro.

SEGURIDAD DE SISTEMAS DE INFORMACION

Política: El área de sistemas tiene como una de sus funciones la de proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como los backup de datos de información automatizados.

Las políticas y estándares de seguridad informática tienen por objeto establecer medidas y patrones técnicos de administración y organización de las Tecnologías de Información y Comunicaciones TIC´s de todo el personal comprometido en el uso de los servicios informáticos proporcionados por el área de sistemas,

También se convierte en una herramienta de difusión sobre las políticas y estándares de seguridad informática a todo el personal de Hospital Facilitando una mayor integridad, confidencialidad y confiabilidad de la información generada por la Oficina

Nuevas Tecnologías al personal, al manejo de los datos, al uso de los bienes informáticos tanto de hardware como de software disponible, minimizando los riesgos en el uso de las tecnologías de información

RESPONSABLE: Ingeniero de Sistemas

VIOLACIONES DE SEGURIDAD INFORMÁTICA

- ✓ Está prohibido el uso de herramientas de hardware o software para violar los controles de seguridad informática. A menos que se autorice por el área de sistemas.
- ✓ Ningún usuario del Hospital debe probar o intentar probar fallas de la Seguridad Informática conocidas, a menos que estas pruebas sean controladas y aprobadas por el área de sistemas.
- ✓ No se debe intencionalmente escribir, generar, compilar, copiar, coleccionar, Políticas y Estándares de Seguridad Informática, ejecutar o intentar introducir cualquier tipo de código (programa) conocidos como virus, gusanos o caballos de Troya, diseñado para auto replicarse, dañar o afectar el desempeño o acceso a las computadoras, redes o información del Hospital.

  RESPONSABLE: Ingeniero de Sistemas

CONTROL DE ACCESOSREMOTOS

La administración remota de equipos conectados a Internet no está permitida, salvo que se cuente con el visto bueno y con un mecanismo de control de acceso seguro autorizado por el dueño de la información y del área de sistemas y la Gerencia del Hospital.

RESPONSABLE: Ingeniero de Sistemas, auxiliares de sistemas y personal autorizado por la gerencia

CONTROLES DE ACCESO LÓGICO

- ✓ Todos los usuarios de servicios de información son responsables por el de usuario y contraseña que recibe para el uso y acceso de los recursos.

- ✓ Todos los usuarios deberán informar los mecanismos de control de acceso provistos por el área de sistemas antes de poder usar la infraestructura tecnológica del hospital
- ✓ Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica de del hospital, a menos que se tenga el visto bueno Políticas y Estándares de Seguridad Informática.

RESPONSABLE: Ingeniero de Sistemas

SEGURIDAD HARWARE, SOFTWARE Y REDES

5. **PROCEDIMIENTO SEGURIDAD DE LA RED INALAMBRICA**:

- ✓ Para la red inalámbrica se tiene la seguridad por registro de ip, registro de mac, y se tiene clave de acceso no podrá entrar a l red inalámbrica e internet ningún equipo de cómputo o móvil que llegue al hospital y quiera acceder a menos que llegue a sistema para su registro en donde se llenan los datos de la persona nueva o temporal.
  RESONSABLE: Ingeniero de Sistemas

6. ADMINISTRACIÓN DE LA RED

- ✓ Los usuarios de las áreas del hospital no deben establecer redes de área local, conexiones remotas a redes internas o externas, intercambio de información con otros equipos de cómputo utilizando el protocolo de transferencia de archivos (FTP), u otro tipo de protocolo para la transferencia de información empleando la infraestructura de red del hospital, sin la autorización del área de sistemas.
- ✓ EL hospital en cada computador tiene activo el firewalls la red esta unificada por grupos de trabajo según el área y se encuentra segmentada en varias áreas con el fin de mantener una integralidad de la información.
  RESONSABLE: Ingeniero de Sistemas

SEGURIDAD PARA LA RED

Será considerado como un ataque a la seguridad informática y una falta grave, cualquier actividad no autorizada por el área de sistemas, en la cual los usuarios o funcionarios realicen la exploración de los recursos informáticos en la red del hospital,

así como de las aplicaciones que sobre dicha red operan, con fines de detectar y explotar una posible vulnerabilidad.

7. **REDES DE DATOS CABLEADA E INALAMBRICA:** Para la red inalámbrica y cableada se tiene un archivo con las direcciones ip en donde antes de la asignación de un equipo a un usuario se verifica que no esté repetida y que pueda ser asignada.

8. **EL ROUTER Y LA SEGURIADAD** El área tesorería se encuentra aislado por seguridad de los datos en donde se trabaja con el portal del banco y tiene asignado una ip fija en donde nadie puede acceder a ella.

9. **SWITCHES:** Uno se encuentra en sistemas y los otros dos en la oficina de estadística, dentro de un gabinete para evitar el polvo y la humedad y están protegidos con ups para evitar los bajones de energía, el de sistemas tiene malla a tierra y está pegado toda el área de sistemas a la subestación de energía con una línea independiente.
   RESPONDABLE: Ingeniero de sistemas

SEGURIDAD SISTEMA OPERATIVO

10. **ANTIVIRUS:** Todos los equipos antes de trabajar con ellos el usuario se les instala un antivirus gratuito.

11. **ENTRADA AL SISTEMAWINDOWS:**Cada usuario nuevo en el sistema de cómputo debe entrar con la clave al sistema operativo por una cuenta invitado nadie excepto los de sistemas pueden entrar a instalar o a modificar programas sin previa autorización.

    RESPONSABLES: Usuarios del sistema

SEGURIDAD DEL SISTEMA DE INFORMACION

- ✓ Solo el sistema de información es modificado por los jefes de área los cuales tienen el permiso previamente asignado en su módulo, la clave master solo la tiene el ingeniero de sistemas y solo la empresa Sinergia hace las modificaciones respectivas al sistema si hay un contrato de actualización que lo respalde, o por un correo electrónico que sirva como respaldo para cualquier reclamo.
  RESPONSABLE: Ingeniero de Sistemas

SEGURIDAD FISICA AL CENTRO DE CÓMPUTO

- **PROCEDIMIENTO PARA LA ENTRADA Y SALIDA DEL PERSONAL DE SISTEMAS:**

  Para la entrada en la puerta se tiene un candado en los que solo el personal encargado tiene llave de esa puerta, cada vez que la oficina va a quedar sola se debe cerrar y por ningún motivo se debe dejar abierta a si sea que el personal no se demora en la actividad fuera que realice.

  RESPONSABLES: Ingeniero de Sistemas y auxiliar 1 y 2

- **ADMINISTRACIÓN DE OPERACIONES EN LOS CENTROS DE CÓMPUTO**

  - ✓ Política: Los usuarios y funcionarios deberán proteger la información utilizada en la infraestructura tecnológica de Hospital. De igual forma, deberán proteger la información reservada o confidencial que por necesidades institucionales deba ser guardada, almacenada o transmitida, ya sea dentro de la red interna institucional a otras dependencias de sedes alternas o redes externas como internet.

  - ✓ Los usuarios y funcionarios de Hospital que hagan uso de equipos de cómputos, deben conocer y aplicar las medidas para la prevención de código malicioso como pueden ser virus, caballos de Troya o gusanos de red.

  - ✓ El Área de sistemas en cabeza del Jefe de Sistemas, establece las políticas y procedimientos administrativos para regular, controlar y describir el acceso de visitantes o funcionarios no autorizados a las áreas funcionales del hospital restringidas.

  - ✓ Todo equipo informático ingresado al area de sistemas restringidos deberá ser registrado en el libro de visitas.
  - ✓ Cuando se vaya a realizar un mantenimiento en algunos de los equipos del Centro de Cómputo restringido, se debe dar aviso con anticipación a los usuarios para evitar traumatismos.
  - ✓ El Jefe del area de sistemas deberá solicitar a la gerencia los equipos de protección para las instalaciones contra incendios,

  RESPONSABLE DE LA ENTRADA: Auxiliar de sistemas 1, Auxiliar de Sistemas 2, ingeniero de Sistemas.

EQUIPOS DE CÓMPUTO

- **PROCEDIMIENTO SEGURIDAD EQUIPOS DE COMPUTO**
  A los equipos de cómputo se les hace mantenimiento preventivo trimestralmente,
  RESPONSABLE DEL MANTENIMIENTO DE EQUIPOS: Auxiliar de sistemas 1

RED ELECTRICA

- **LA RED ELECTRICA DE LOS COMPUTADORES:** El área de Mantenimiento en el caso de que se tenga algún inconveniente con algún toma de los router computadores o demás instalaciones eléctricas el área encargada es el área de mantenimiento.

  RESPONSABLE DEL MANTENIMIENTO DE LA RED ELCTRICA: Es el área de Mantenimiento y el responsable es el jefe inmediato del área.

USO DEL INTERNET

El acceso a Internet provisto a los usuarios y funcionarios de Hospital es exclusivamente para las actividades relacionadas con las necesidades del cargo y funciones desempeñadas.

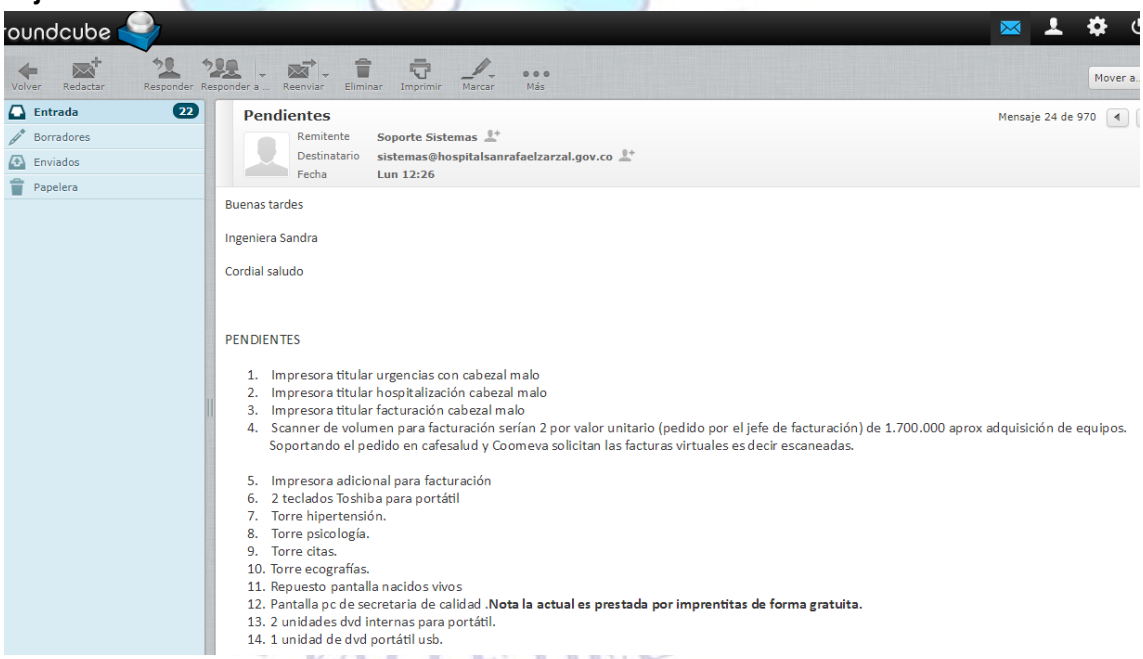
- ✓ Todos los accesos a Internet tienen que ser realizados a través de los canales de acceso provistos por el Hospital, en caso de necesitar una conexión a Internet alterna o especial, ésta debe ser notificada y aprobada por el area de sistemas.
- ✓ Los usuarios de Internet del Hospital tienen que reportar todos los incidentes de seguridad informática al area de sistemas inmediatamente después de su identificación, indicando claramente que se trata de un incidente de seguridad informática.
- ✓ Los usuarios del servicio de navegación en Internet, al aceptar el servicio están aceptando que Serán sujetos de monitoreo de las actividades que realiza en Internet, saben que existe la prohibición al acceso de páginas no autorizadas, saben que existe la prohibición de transmisión de archivos reservados o confidenciales no autorizados. Saben que existe la prohibición de descarga de software sin la autorización del area de sistemas. La utilización de Internet es para el desempeño de sus funciones y cargo en el Hospital y no para propósitos personales.

RESTRICCIONES PARA EL ACCESO A INTERNET

- El área de sistemas instala en los equipos de cómputo el archivo host con las paginas prohibidas para que el usuario no acceda sin autorización, se crea una cuenta invitado y administrador para que no lo modifiquen y no puedan ver ni instalar los DNS para internet .
- Para la acceder a la red inalámbrica el router está con filtrado de mac y con una ip estática que tiene que ser consultada al área de sistemas para poder instalarla.
- Se coloca nombres raros para que no se encuentre fácil la red.
- El acceso a internet está restringido para personas de fuera del hospital a menos que la gerencia autorice.
- Se cambia constantemente la puerta de enlace para evitar instrusos.

- **SOLCITUD DE PEDIDOS**

Los pedidos de sistemas se hacen por correo electrónico al area administrativa
Adjunto: 2015-2017



Se envían adjunto listado de pendientes y se va solicitando en correo la viabilidad de la compra sea un insumo o una solicitud de un servicio.

- **CONTROLES EN LA COMPRA DE COMPUTADORES**

ANEXO: POLITICAS DE COMPRA DE EQUIPOS

➢ USO DE DISPOSITIVOS EXTRAÍBLES

- ✓ El área de sistemas, velará porque todos los usuarios de los sistemas de Información estén registrados en su Base de Datos para la autorización de uso de dispositivos de almacenamiento externo, como Pen Drives o Memorias USB, Discos portátiles, Unidades de Cd y DVD Externos, para el manejo y traslado de información o realización de copias de seguridad o Backups.
- ✓ Cada Jefe de Área o dependencia debe reportar al area de sistemas el listado de funcionarios a su cargo que manejan estos tipos de dispositivos, especificando clase, tipo y uso determinado.
- ✓ El uso de los quemadores externos o grabadores de disco compacto es exclusivo para Backups o copias de seguridad de software y para respaldos de información que por su volumen así lo justifiquen.
- ✓ El servidor o funcionario usuario que tengan asignados estos tipos de dispositivos serán responsable del buen uso de ellos.
- ✓ Si algún área o dependencia por requerimientos muy específicos del tipo de aplicación o servicios de información tengan la necesidad de contar con uno de ellos, deberá ser justificado y autorizado por el area de sistemas con el respectivo visto bueno de la gerencia o en su defecto de su Jefe inmediato o un superior

➢ PÉRDIDA DE EQUIPO

- ✓ El servidor o funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

- ✓ El préstamo de portátiles tendrá que solicitarse al area de sistemas, con el visto bueno del encargado de sistemas.

- ✓ El servidor o funcionario deberán dar aviso inmediato al area de sistemas, y a l a Administración de Inventarios de Activos de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

- **MANTENIMIENTO DE EQUIPOS**

  - ✓ Únicamente el personal autorizado por el area de sistemas podrá llevar a cabo los servicios y reparaciones al equipo informático.

  - ✓ Los usuarios deberán asegurarse de respaldar en copias de respaldo o backups la información que consideren relevante cuando el equipo sea enviado a reparación y borrar aquella información sensible que se encuentre en el equipo, previendo así la pérdida involuntaria de información, derivada del proceso de reparación

  - **PROTECCIÓN Y UBICACIÓN DE LOS EQUIPOS**

- ✓ Los usuarios no deben mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del área de sistemas en caso de requerir este.

- ✓ El Área de Inventarios de activos o almacén será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por el area de sistemas

- ✓ El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones de los funcionarios o servidores del hospital.

- ✓ Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas informáticas que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.

- ✓ Es responsabilidad de los usuarios almacenar su información únicamente en la partición del disco duro diferente destinada para archivos de programas y sistemas operativos, generalmente c:\.

- ✓ Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.

- ✓ Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.

- ✓ Se debe mantener el equipo informático en un lugar limpio y sin humedad.

- ✓ El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos encima o contra ellos en caso de que no se cumpla solicitar un reubicación de cables con el personal del área de sistemas.

- ✓ Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con tres días de anticipación a el área de sistemas a través de un plan detallado.

- ✓ Queda terminantemente prohibido que el usuario o funcionario distinto al personal del área de sistemas abra o destape los equipos de cómputo.

➢ **CONTROLES DE ACCESO FÍSICO**

- ✓ Cualquier persona que tenga acceso a las instalaciones del hospital, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente.

- ✓ Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá ser retirado de las instalaciones del hospital únicamente con la autorización de salida del área de sistemas.

- ✓ El acceso al centro de cómputo está restringido por un letrero y solo entra el personal que está autorizado.

➢ **PROTECCIÓN DE LA INFORMACIÓN Y DE LOS BIENES INFORMÁTICOS**

- ✓ El usuario o funcionario deberán reportar de forma inmediata al área de sistemas cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

- ✓ El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

- ✓ Es responsabilidad del usuario o funcionario evitar en todo momento o la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo personal que tenga asignados.

➢ PROTECCIÓN DE LA INFORMACIÓN Y DE LOS BIENES INFORMÁTICOS

- ✓ El usuario o funcionario deberán reportar de forma inmediata al area de sistemas cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.

- ✓ El usuario o funcionario tienen la obligación de proteger las unidades de almacenamiento que se encuentren bajo su responsabilidad, aun cuando no se utilicen y contengan información confidencial o importante.

➢ SANCIONES

- ✓ Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de esta dependencia, o de que se le declare culpable de un delito informático

➢ CAPACITACIÓN EN SEGURIDAD INFORMÁTICA

- ✓ Todo servidor o funcionario nuevo en en el hospital deberá contar con la inducción sobre las Políticas y Estándares de Seguridad Informática Manual de Usuarios, donde se den a conocer las obligaciones para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

- **OBLIGACIONES DE LOS USUARIOS**
  - ✓ Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir las Políticas y Estándares de Seguridad Informática para Usuarios del presente Manual.
- **USUARIOS NUEVOS**

✓ Todo el personal nuevo de del hospital, deberá ser notificado al área de sistemas, para asignarle los derechos correspondientes (Equipo de Cómputo, Creación de Usuario para la Red (Perfil de usuario en el Directorio Activo) o en caso de retiro del funcionario, anular y cancelar los derechos otorgados como usuario informático.

- **EQUIPO DESATENDIDO**

Los usuarios deberán mantener sus equipos de cómputo con controles de acceso como contraseñas y protectores de pantalla previamente instalados y autorizados por el área de sistemas cuando no se encuentren en su lugar de trabajo.

- **SEGURIDAD INSTITUCIONAL**

✓ Política: Toda persona que ingresa como usuario nuevo al hospital para manejar equipos de cómputo y hacer uso de servicios informáticos debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en el Manual de Políticas y Estándares de Seguridad Informática para Usuarios.

- **EVALUACIÓN DE LAS POLÍTICAS**

✓ Las políticas tendrán una revisión periódica se recomienda que sea semestral para realizar actualizaciones, modificaciones y ajustes basados en las recomendaciones y sugerencias

- **PLANES DE CONTINGENCIA ANTE DESASTRE**

ANEXO: PLAN DE CONTINGENCIA INFORMATICO
Definición: Se entiende por PLAN DE CONTINGENCIA los procedimientos alternativos a la operación normal en una organización, cuyo objetivo principal es permitir el continuo funcionamiento y desarrollo normal de sus operaciones, preparándose para superar cualquier eventualidad ante accidentes de origen interno o externo, que ocasionen pérdidas importantes de información. Estos deben prepararse de cara a futuros sucesos, Ver Manual de Contingencias.

Con el fin de asegurar, recuperar o restablecer la disponibilidad de las aplicaciones que soportan los procesos de misión crítica y las operaciones informáticas que soportan los servicios críticos de la Institución, ante el evento de un incidente o catástrofe parcial y/o total.

CONTROLES PARA LA GENERACIÓN Y RESTAURACIÓN DE COPIAS DE RESPALDO (BACKUPS)

Procedimiento de generación y restauración de copias de respaldo para salvaguardar la información crítica de los procesos significativos de la entidad. Se deberán considerar como mínimo los siguientes aspectos:

- Establecer como medida de seguridad informática la necesidad de realizar copias de respaldo o backups periódicamente en los equipos de cómputo administrativos y servidores. Se pasaran a un disco duro externo diariamente y también se hace automáticamente 4 copias. El área de sistemas es la responsable de realizar las copias del sistema sihos.

- Cada funcionario es responsable directo de la generación de los backups o copias de respaldo, asegurándose de validar la copia. También puede solicitar asistencia técnica para la restauración de un backups.

- Conocer y manejar el software utilizado para la generación y/o restauración de copias de respaldo, registrando el contenido y su prioridad. Rotación de las copias de

respaldo, debidamente marcadas. Almacenamiento interno o externo de las copias de respaldo, o verificar si se cuenta con custodia para ello.

- Se utilizará el programa Nero Express en la opción Copia de Seguridad o Back Up: Aplicación PC, Copiar Disco⎪ Opción Datos: se escoge CD o DVD⎪

- Se añaden los archivos o carpetas Clic en cerrar⎪ Clic en siguiente⎪ Se introduce un CD o DVD en blanco en la unidad quemador de CD o DVD⎪ Colocar nombre al disco (16 caracteres)⎪ Si la información no abarca 700 megas en CD o 4.3 gigas en DVD se habilita⎪ la pestaña: Permitir añadir archivos posteriormente. Clic en grabar⎪ Marcar el CD o DVD colocándole la fecha de la copia y entregar a su Jefe⎪ inmediato para su almacenamiento y custodia.

- Las copias de seguridad o Back ups se deben realizar al menos una vez a la semana y el último día hábil del mes. Un funcionario del área de sistemas revisará una vez por semana, el cumplimiento de este procedimiento y registrará en el formato de Copias de Seguridad.

- **ALMACENAMIENTO PARA EL RESGUARDO DE PROGRAMAS Y ARCHIVOS DE DATOS**

  En el servidor se realizan copias de seguridad diarias de las cuales se van a un disco duro diferente donde se encuentra la información general del sistema y se sacan a un disco duro externo por si hay algún daño total del equipo luego se entregan archivo central para la salvaguarda.
  RESPONSABLE: Ingeniero de sistemas
  ANEXO:SALVA GUARDA DE LA INFORMACIO

- **CONTROLES CONTRA VIRUS O SOFTWARE MALICIOSO**

  - ✓ Para revisar si el antivirus se actualiza correctamente, seleccione el icono de su programa antivirus Nod32 , toda memoria que se coloque en el puerto usb del computador debe ser vacunada.

  Se vacuna con software gratuito para evitar compra de licencias.

- **USO DEL CORREO ELECTRÓNICO**

- ✓ Los usuarios y funcionarios no deben usar cuentas de correo electrónico asignadas a otras personas, ni recibir mensajes en cuentas de otros. Si fuera necesario leer el correo de alguien más (mientras esta persona se encuentre fuera o de vacaciones) el usuario ausente debe redireccionar el correo a otra cuenta de correo interno, quedando prohibido hacerlo a una dirección de correo electrónico externa al hospital, a menos que cuente con la autorización del area de sistemas.

- ✓ Los usuarios y funcionarios deben tratar los mensajes de correo electrónico y archivos adjuntos como información de propiedad del hospital. Los mensajes de correo electrónico deben ser manejados como una comunicación privada y directa entre emisor y receptor.

- ✓ Los usuarios podrán enviar información reservada y/o confidencial vía correo electrónico siempre y cuando vayan de manera encriptado y destinada exclusivamente a personas autorizadas y en el ejercicio estricto de sus funciones y responsabilidades.

- ✓ Queda prohibido falsificar, esconder, suprimir o sustituir la identidad de un usuario de correo electrónico.

- ✓ Queda prohibido interceptar, revelar o ayudar a terceros a interceptar o revelar las comunicaciones electrónicas.

- ✓ **IDENTIFICACIÓN DEL INCIDENTE**

  - ✓ El usuario o funcionario que detecte o tenga conocimiento de la posible ocurrencia de un incidente de seguridad informática deberá reportarlo al Área de sistemas lo antes posible, indicando claramente los datos por los cuales lo considera un incidente de seguridad informática.

  - ✓ Cuando exista la sospecha o el conocimiento de que información confidencial o reservada ha sido revelada, modificada, alterada o borrada sin la autorización de las Directivas Administrativas

competentes, el usuario o funcionario informático deberá notificar a la área de sistemas.

- ✓ Cualquier incidente generado durante la utilización u operación de los activos de tecnología de información del hospital debe ser reportado a área de sistemas.

➢ USO DE MEDIOS DE ALMACENAMIENTO

Los usuarios y servidores del hospital deben conservar los registros o la información que se encuentra activa y aquella que ha sido clasificada como reservada o confidencial.

Las actividades que realicen los usuarios y funcionarios en la infraestructura Tecnología de Información y Comunicaciones (TIC´s) del hospital serán registradas y podrán ser objeto de auditoria.

AREA DE SISTEMAS DE INFORMACION