HOSPITAL DEL SARARE
Empresa Social del Estado
Evolucionamos pensando en usted

Sistema Integrado de Gestión

Manual

MANUAL DE POLITICAS DE SEGUIRIDAD DE LA INFORMACIÓN

Gestión de la Información

TRD. 322.1.28.126

TABLA DE CONTENIDO

TRD. 322.1.28.126

TRD. 322.1.28.126

1. INTRODUCCION

La ESE HOSPITAL DEL SARARE, identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la entidad, razón por la cual es necesario que la ESE establezca un marco en el cual se asegure que la información es protegida de una manera adecuada independientemente de la forma en la que ésta sea manejada, procesada, transportada o almacenada.
Este documento describe las políticas y normas de seguridad de la información definidas para la ESE. Para la elaboración del mismo, se toman como base las leyes y demás regulaciones aplicables, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013
La seguridad de la información es una prioridad para LA ESE y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2. GENERALIDADES

2.1. Objetivo del manual

Esta guía de buenas prácticas o manual, integra políticas que trazan las directrices y las acciones que deben seguir los colaboradores del Hospital del Sarare para facilitar el cumplimiento de los objetivos que en materia de tecnología y seguridad informática se ha propuesto.

2.2. Ámbito de Aplicación

El presente manual es aplicable a todos los funcionarios que laboran en el Hospital del Sarare y es responsabilidad de los mismos, proteger los recursos tecnológicos asignados por la institución, así como cumplir y velar por el cumplimiento de las políticas establecidas en el presente manual

2.3. Visión General

Servir de guía y herramienta de permanente consulta, con el fin de cumplir la normatividad establecida por el Hospital del Sarare para la correcta aplicación de la tecnología y la seguridad informática, garantizando que los sistemas no sean vulnerados poniendo en peligro la información confidencial que maneja y por consiguiente los procesos operativos aplicados en las actividades llevadas a cabo apoyando la continuidad del negocio

2.4. Apoyo tecnológico

Como apoyo tecnológico, se cuenta con los equipos de computación, sistemas de comunicaciones, sistemas para cifrar datos, sistemas de detección de intrusión, firewall y administración, entre otros, los cuales facilitan el manejo y el control de la información, la seguridad y la confidencialidad de la misma

3. MARCO DE REFERENCIA

3.1. Antecedentes.

TRD. 322.1.28.126

Antecedentes Teniendo en cuenta que la información es un activo vital para el éxito y el cumplimiento de la misión de la ESE HOSPITAL DEL SARARE, este documento se encuentra alineado con la familia de normas de la serie ISO 27000 como marco de referencia para la implementación de su sistema de gestión de Seguridad de la Información.

ISO 27000 es un conjunto de estándares desarrollados por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión de la Seguridad de la Información utilizable por cualquier tipo de organización. Entre las distintas normas que componen la serie ISO 27000 y que fueron tomadas como referente, se resalta ISO/IEC 27001 sobre los requisitos para el establecimiento del sistema de gestión de Seguridad de la Información.

La información, así como la plataforma tecnológica que la soporta, es considerada un activo estratégico para la ESE HOSPITAL DEL SARARE, por lo que es fundamental establecer políticas que definan el marco de control para brindar seguridad a los activos de información de la Entidad. Estos activos de información se constituyen en el soporte de la misión y la visión, por lo que requieren ser utilizados y manejados dentro de un adecuado entorno de seguridad, cualquiera que sea el medio y el ambiente tecnológico en el que se encuentren.

Hoy por hoy, las organizaciones tanto públicas como privadas se están tornando altamente dependientes de sus sistemas de información y de los recursos informáticos que los soportan, por lo que se convierte en una decisión estratégica el implementar un Sistema de Gestión de Seguridad de la Información que esté directamente relacionado con las necesidades, objetivos institucionales y direccionamiento estratégico.

La implementación de un Sistema de Gestión de Seguridad de la Información está orientada a definir los aspectos necesarios para establecer, operar, mantener y dirigir de manera estandarizada, sistemática y organizada un sistema efectivo que permita el tratamiento seguro de la información.

3.2. **Referencias Normativas**

- Ley 1266 de 2008 “Por lo cual se dictan las disposiciones generales del habeas data y se regula el manejo de la información”.
- Ley 1273 de 2009 “Protección de la Información y de los Datos”.
- Documento CONPES 3701 de julio del 2011 “Lineamientos de política para ciberseguridad y ciberdefensa”.
- Ley 1581 de 2012 “Por la cual se dictan disposiciones generales para la protección de datos personales” y su decreto reglamentario 1377 del 27 de junio de 2013.
- Manual para la implementación de la Estrategia de Gobierno en Línea en las entidades del orden nacional de la Republica de Colombia.
- Norma Técnica Colombiana NTC – ISO/IEC 27000

TRD. 322.1.28.126

4. TÉRMINOS Y DEFINICIONES

- **Ambiente Computacional:** Conjunto de recurso (hardware y software) que integrado proveen aplicación informática

- **Backup:** Información de respaldo de archivos, base de datos en medios magnéticos

- **Inventario de activos**: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

- **ISO**: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares

- **ISO 27001:** Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

- **Plan de continuidad del negocio (Bussines Continuity Plan):** Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

- **Política de seguridad:** Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

- **Seguridad de la información**: Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas. Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

- **SGSI Sistema de Gestión de la Seguridad de la Información**: Según [ISO/IEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

- **Servicios de tratamiento de información**: Según [ISO/IEC 27002:2013]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

TRD. 322.1.28.126

- **Clasificación de los Sistemas:**

  - ✓ **Sistemas Misionales:** Son aquellos que son vitales para la continuación del negocio y que siempre tienen que estar en funcionamiento y lo comprenden los diferentes sistemas de información que tiene la empresa

  - ✓ **Sistemas de Apoyo:** Aplicaciones utilizadas para la administración, operación y control institucional. Hace referencia a los procesadores de palabras, hojas de cálculos, etc

- **Comunicaciones:**

  - ✓ **Seguridad Perimetral:** Es un sistema de seguridad enfocado a controlar una red dividida en unidades lógicas desde una central, utilizando diferentes tipos de herramienta (hardware o software) que detecten y avisen de cualquier intrusión o violación a los perímetros establecidos

  - ✓ **Firewall:** Sistema de seguridad que impide el acceso de personas no autorizadas a una red interna desde el exterior

- **Disclaimers:** Normas de confidencialidad para mantener la privacidad dela información, obtenida a través de los medios de correos electrónicos e internet

- **Dispositivos:** Mecanismo, maquina o aparato dispuesto para producir una función determinada

  - ✓ **Dispositivos de almacenamiento removible:** dispositivo para el almacenamiento de información dentro de los cuales se encuentran: memorias flash (USB, SD, Mini SD), cámaras digitales, reproductores mp3/mp4/mp5 discos duros portables, agendas digitales personales (PDA), teléfonos celulares, ipod, iphone, ipad, discos ópticos (CD, DVD), entre otros dispositivos que permiten que permiten el almacenamiento de información

✓ **Información confidencial:** Número de identificación y nombre de los pacientes con la información detallada de los diferentes procedimientos que reposa en la historia clínica

  - ✓ **Criterio de seguridad de la información:**

    - ❖ **Confidencialidad:** Concierne a la protección de información confidencial

    - ❖ **Disponibilidad:** Relación con la información para que esté disponible cuando sea requerida por los procesos del negocio. También concierne a la salvaguardia de los recursos y sus capacidades asociadas

TRD. 322.1.28.126

- ❖ **Integridad:** La información debe ser exacta, valida, precisa, coherente y completa desde su creación hasta su destrucción

✓ **Criterio de seguridad de calidad:**

- ❖ **Confiabilidad:** Se refiere a que los sistemas proveen a la administración información apropiada para la operación del negocio y dando cumplimiento a las diferentes responsabilidades con los organismos de control
- ❖ **Cumplimiento:** Tiene que ver con estar de acuerdo con aquellas leyes, regulación y obligaciones contractuales a las cuales está sujeto el proceso del negocio
- ❖ **Efectividad:** se refiere a que la información sea relevante y pertinente para los procesos del negocio, así como que sea entregada de una manera oportuna, correcta, consistente, utilizable y completa
- ❖ **Eficiencia:** Concierne al suministro de información a través del uso óptimo (más productivo y económico) de los recursos de tecnología informática

✓ **Log:** (Rastro o pista de auditoria) es un registro que contiene evidencia sobre los eventos o acciones presentados sobre un sistema. Por ejemplo: intentos de adivinar una contraseña, intentos para usar privilegios que no han sido autorizados, modificaciones al software de aplicación, modificaciones a los sistemas operativos, modificaciones y acceso a la información

✓ **Evidencia Digital:** Es un tipo de evidencia física que puede tomar muchas como son:

- ❖ Registro de aplicaciones, sistema operacional, comunicaciones (logs de transacciones, logs de seguridad, logs de intentos de login fallidos, entre otros)
- ❖ Imágenes o graficas
- ❖ Documentos en todos los formatos
- ❖ Correos Electrónicos y faxes
- ❖ Información financiera y de transiciones
- ❖ Archivos de cache, cookies
- ❖ Archivos eliminados
- ❖ Archivo de intercambio

Mapa de riesgo: Es una metodología para determinar el nivel de riesgo informático al que está expuesto el negocio y sus unidades funcionales, sirve como soporte a la elaboración de un plan de acción de orden preventivo, activo y correctivo, que permite la reducción significativa del riesgo

TRD. 322.1.28.126

- ✓ **Modems:** Equipo de comunicaciones que permite transmitir y recibir datos a través de un medo analógico. Durante la transmisión, hace la conversión de análogo a digital para que pueda ser interpretada por los equipos informáticos (computadores estaciones de trabajo)

- ✓ **Operaciones:** Son las acciones a través de las cuales se desarrollan, ejecutan o materializan los productos o servicios que presta el hospital a toda la población

- ✓ **Riesgo informático:** incertidumbre que tiene sobre la ocurrencia de un evento informático no esperado que puede ser medido en términos probabilísticos tanto su ocurrencia, como la gravedad de su posible consecuencia

- ✓ **Seguridad en sistemas operativos:**

  Entre las seguridades aplicadas a los sistemas operativos se tienen:

  - ✓ **Plan de auditoria:** Mecanismo de verificación y control para garantizar los principios básicos de confidencialidad, integridad, autenticidad y disponibilidad de la información

  - ✓ **Plan de cuentas:** Plan cuyo objetivo es definir como los usuarios interactúan con los sistemas en el instante del ingreso al mismo. Se configura estableciendo una serie de parámetros en el sistema que se ejecuta sobre este, en donde se definen características como: vigencia de la cuenta, vigencia de la clave de acceso, horario de trabajo, histórico de clave de acceso, estado de la cuenta, disco o volumen por defecto, periodo de gracia para el cambio de clave de acceso, longitud mínima de la clave de acceso, cambio de la clave de acceso por parte del usuario, numero de intentos fallidos antes de bloquear la cuenta, tiempo de bloqueo de una cuenta por exceder un numero de intentos fallidos de acceso, definición de terminales donde el usuario puede acceder al sistema, histórico de la clave antes de volver a utilizar una clave ya usada

  - ✓ **Puerta trasera:** son entradas no convencionales (no controladas) a los sistemas operacionales que permiten acceso a intrusos sin que puedan ser detectados; además, pueden afectar algunos recursos del sistema que al ser utilizados por otros procesos validos generen un hueco de mayor tamaño en la seguridad del sistema. Los intrusos o hacker desarrollan técnicas muy poderosas para obtener acceso a los sistemas por encima de las labores de seguridad que los administradores efectúan. Se debe aceptar la existencia de estas puertas en la mayoría de los sistemas operacionales y efectuar las tareas necesarias para contrarrestar la vulnerabilidad que ellas generan

- ✓ **Seguridad informática:** Medidas de protección contra riesgos inherentes a la plataforma informática y que pueden afectar la integridad, disponibilidad y confidencialidad de la información

TRD. 322.1.28.126

- ✓ **Servicio de acceso remoto (RAS)** Es la posibilidad de ingresar a los sistemas de información de la institución desde una red o un lugar externo utilizando enlaces dedicados o conmutados

- ✓ **Sniffers:** Sistemas basados en hardware y/o software que se usa para capturar datos que viajan dentro de una red local, para propósitos de análisis y diagnóstico de problemas de protocolos

- ✓ **Vulnerabilidad informática:** ausencia o deficiencia que permite violar las medidas de seguridad informáticas para poder acceder a un canal de distribución o a un sistemas especifico de formas no autorizada y emplearlo en beneficios propios o como origen de ataques por parte de tercero

5. POLITICAS

Para aplicar la normatividad incluida en el presente manual, así como para aclaración de dudas al respecto, contacte la oficina de sistemas.

5.1. Responsabilidades

5.1.1. De los funcionarios

Todos los funcionarios a quien está dirigido la normatividad están obligados a cumplir y velar por su cumplimiento.

5.1.2. Auditoria de sistemas

Efectuar revisión y seguimiento permanente sobre el cumplimiento de esta normatividad

5.1.3. Áreas responsables de colocarla en operación

Todas las áreas del hospital tienen la responsabilidad de colocar en operación las políticas desarrollando las normas, procedimientos y demás instrumentos definidos que permitan su efectiva aplicación.

5.2. Política de administración de seguridad informática – funciones y responsabilidades de la oficina de sistemas

5.2.1. Funciones y responsabilidades generales

La oficina de sistemas es la responsable de:

1. Definir, implementar, controlar y mantener las políticas, normas, estándares, procedimiento, funciones y responsabilidades necesarias para preservar y proteger la confidencialidad, disponibilidad e integridad de la información del hospital, en donde esta resida (aplicaciones, bases de datos, sistemas operativos, redes, backup y otros medios).

TRD. 322.1.28.126

2. Propender por alinear las estrategias de seguridad informática con planes estratégicos y de operación del hospital

3. Autorizar las excepciones a las políticas de seguridad, de las cuales se debe dejar constancia delos riesgos que en forma consciente se están asumiendo y el periodo de vigencia de la excepción.

4. Igualmente, es la encargada de definir la “Arquitectura de seguridad” para el hospital y facilitar la incorporación de prácticas de seguridad de la información en todas las dependencias.

5. Establecer e implementar un plan de seguridad informática que permita controlar el entorno lógico y físico de la “Información estratégica del hospital”, teniendo en cuenta los criterios de confidencialidad, integridad, auditabilidad, disponibilidad, autenticidad y no repudio de la información.

6. Participar activamente en los proyectos informativos del hospital para proveerlos de la seguridad informática adecuadas.

7. Contar con mecanismo de monitoreo con el fin de detectar oportunamente procedimiento inseguro para los sistemas operacionales, aplicativos, datos y redes.

8. Implementar procedimientos que permitan verificar que la información enviada esté libre de software malicioso.

9. Monitorear los sistemas de seguridad de la información y reportar periódicamente su efectividad.

10. Promulgar la cultura de “seguridad informática” a todos los usuarios a través de informativos, videos, cartillas, entre otros.

11. Proponer por que el hospital cuente con ambientes indispensables de desarrollo, prueba y producción en sus ambientes de misión crítica y prioritaria.

12. Velar porque los mantenimientos a los sistemas informáticos sean autorizados, probados e implementados de acuerdo con los requerimientos de los usuarios y que no comprometan la seguridad informática del hospital. Además, que los sistemas de información queden correctamente documentados y se dé la capacitación necesaria a los usuarios finales.

13. Custodiar las llaves informáticas del hospital y velar porque la generación de las mismas sean realizadas de acuerdo con el procedimiento establecido (minimo en dos (2) partes

independiente cada una de no menos de ocho (8) caracteres). Los custodios del hospital son en su orden, oficina de sistemas y auditoria de sistemas.

14. Efectuar pruebas periódicas de penetración a los sistemas de redes y computación del hospital.

5.2.2. Elaboración del mapa de riesgo

Es responsabilidad de la oficina de sistemas efectuar estudios periódicos de análisis de riesgos en “seguridad informática” para identificar oportunamente os eventos o situaciones que atenten contra la integridad, confidencialidad, auditabilidad y disponibilidad de la información presentados en el hospital, estableciendo planes de acción que incluyan controles para contrarrestarlos y reducir el riesgo a un nivel aceptable.

5.2.3. Capacitación y entrenamiento

La oficina de sistemas establece y apoya a las áreas encargadas en la ejecución de un plan de capacitación continuo que permita actualizara los funcionarios en aspectos de “seguridad informatice” fortaleciendo la cultura sobre el tema.

5.3. Políticas de personas

Se relaciona a continuación las políticas que los funcionarios del hospital deben seguir para el correcto manejo de los equipos de cómputos asignados a su uso, la protección de la información, así como el control y la responsabilidad que sobre los mecanismos de acceso y claves deben ejercer.

“La responsabilidad por la seguridad de la información no es únicamente de la oficina de sistemas, es una obligación de cada uno de los funcionarios que tiene el hospital”

5.3.1. Códigos de identificación y palabras claves de acceso a los sistemas de información

1. La asignación de claves para el ingreso a los sistemas de información es personalizada.

2. Las palabras claves o los mecanismos de acceso que les sean otorgados a los funcionarios son responsabilidad exclusiva de cada uno de ellos y no deben de ser divulgados a ninguna persona, a menos que exista un requerimiento legal o medie un procedimiento de custodia de claves. De acuerdo con lo anterior, los usuarios no deben obtener palabras claves u otro mecanismo de acceso de otros usuarios que pueda permitirles acceso no autorizados.

3. Los usuarios son responsables de toda actividad llevadas a cabo con su código de identificación de usuario y sus claves personales.

5.3.2. Control de la Información

1. Todo funcionario debe informar oportunamente a la oficina de sistemas acerca de cualquier alteración o modificación no autorizada de los dispositivos, equipos de cómputo, sistemas de información o cualquier elemento de la infraestructura tecnológica.

2. Los usuarios no deben instalar software en sus computadores o en servidores sin las debidas autorizaciones.

3. Los usuarios no deben alterar las configuraciones estándar definidas por la oficina de sistemas, tales como: Perfiles de usuario, protectores de pantalla, entre otros.

4. Los usuarios no deben intentar sobrepasar los controles de los sistemas, examinar los computadores o redes del hospital o introducir intencionalmente software diseñado para causar daño o impedir el normal funcionamiento de los sistemas. Además, todo software que permita realizar monitoreo (sniffers) sobre los computadores y redes deberá estar debidamente autorizada.

5. Los funcionarios no deberán suministrar información del hospital confidencial de los diferentes procesos a ningún ente externo y/o sujeto sin las autorizaciones respectivas.

6. Los funcionarios no deben destruir, copiar o distribuir los archivos del hospital sin los permisos respectivos de la persona responsable del área dueña de la información.

7. Los funcionarios deben velar por la privacidad de la información de los diferentes procesos, de tal manera que no sea distribuida a tercero.

8. Todo funcionario que utilice los recursos de los sistemas, tiene la responsabilidad de velar por la integridad, confidencialidad, disponibilidad y confiabilidad de la información que maneje.

5.3.3. Otros usos

Los computadores, sistemas y otros equipos deben usarse solamente para las actividades propias del hospital, por tanto los usuarios no deben hacer uso de ellos para asuntos personales a menos que exista la respectiva autorización y previa evaluación del riesgo informático de tal labor realizada por la oficina de sistemas.

5.4. Política de Hardware

Se relaciona a continuación las políticas que los funcionarios del hospital deben seguir para la correcta administración, mantenimiento y adquisición de equipos de cómputo y de

telecomunicaciones suministrado por el hospital para el desarrollo de las funciones, de tal manera que se proteja la integridad técnica de la institución.

5.4.1 Adquisición y cambios de Hardware

En el hospital se cuenta con hardware y equipos de telecomunicaciones que permiten prestar los servicios y manejar la información en condiciones de calidad y seguridad.

1. El hardware debe de cumplir con los estándares de tecnología definidos y autorizados por la oficina de sistemas.

2. Cualquier solución tecnológica requiere por el hospital debe ser consultada, evaluada, y autorizada por la oficina de sistemas.

3. Los equipos de cómputo del hospital no deben ser alterados ni mejorados (cambios de procesador, adición de memoria, tarjetas y demás componentes) sin el consentimiento, evaluación técnica y autorización de la oficina de sistemas.

4. Los usuarios deben reportar a los entes pertinentes, sobre daños o pérdida del equipo que tengan a su cuidado y sea propiedad del hospital.

5. Solamente el personal debidamente autorizado por la oficina de sistemas puede realizar el mantenimiento y la instalación o desinstalación de programas o dispositivos en las terminales o equipos de cómputo.

6. Los equipos del hospital deben estar relacionados en un inventario que incluya información de sus características, configuración y ubicación de acuerdo con los parámetros establecido por la oficina de sistemas; los inventarios físicos se deben realizar en forma periódica, regular y eficiente. Cada uno de los equipos debe tener un número de identificación asignado en el proceso de inventario, así como el número de serial del fabricante.

7. El hardware utilizado por el hospital para prestar los servicios debe contar con el soporte de fábrica o proveedor y previa autorización de la oficina de sistemas.

8. Los procesos de alistamiento transporte, mantenimiento, instalación, activación y desactivación de los dispositivos finales utilizando en las áreas de servicios deberán contar con un registro con un registro de las actividades adelantadas sobre los mismo.

9. El traslado o reubicación de los de los equipos de infraestructura tecnológica lo realizara la oficina de sistemas, previa aprobación de las áreas involucradas, reportando el traslado.

5.4.2 Acceso Físico

TRD. 322.1.28.126

1. Los equipos de cómputo, deben estar ubicados en lugares seguros para prevenir alteraciones y uso no autorizado. Se exceptúan los computadores de uso personal, para los cuales cada usuario debe contemplar las medidas de seguridad adecuadas.

2. Las "bibliotecas de cintas magnéticas, discos y documentos" se debe ubicar en sitios acondicionados para tal fin, permitiéndose el acceso únicamente a personas autorizadas.

3. Las conexiones con los sistemas y redes del hospital deben ser dirigidas a través de dispositivos probados por la oficina de sistemas.

4. Las direcciones internas, configuraciones e información relacionada con el diseño de los sistemas de comunicación y cómputo del hospital deben ser de acceso restringido.

5.4.3 Respaldo y Continuidad del Negocio

1. Se debe proveer, mantener y dar entrenamiento a los funcionarios, sobre los sistemas de protección necesarios tales como "sistemas de detección y eliminación de fuego", "sistemas suplementarios de protección eléctrica" y "sistemas de aire acondicionado", entre otros, para asegurar la continuidad del servicio en los sistemas de computación.

2. Los microcomputadores y estaciones de trabajo se deben conectar a unidades suplementarias de energía (UPS), filtros eléctricos, supresores de picos de corriente y en lo posible, eliminadores de corriente estática.

3. La configuración de la red de comunicaciones y de los equipos de cómputo y de seguridad deben estar implementadas de tal forma que garantice su normal operación, por ello se debe evitar tener puntos críticos de falla, como un "centro único de conmutación" que cause la caída de todos los servicios, logrando la continuidad del negocio.

4. A los equipos de cómputo, comunicación y demás equipos de soporte deben realizárseles un mantenimiento periódico preventivo, de tal forma que el riesgo a fallas se mantenga en una probabilidad de ocurrencia baja.

5. El hospital proveerá los recursos y procedimiento disponibles a su alcance con el fin de velar porque los niveles de seguridad de los elementos usados en los canales de transmisión no se vea disminuidos durante toda su vida útil. Dichos procedimientos incluyen, entre otros lo siguientes:

    - Contrato de mantenimiento y/o actualización con proveedores
    - Garantía y reposición o remplazo de elementos y/o equipos usados en los canales de transmisión
    - Monitoreo periódico de los canales de trasmisión

TRD. 322.1.28.126

6. Los planes de contingencia y reparación de equipos deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse.

5.4.4 Dispositivos de almacenamiento removible

1. Todos los equipos de cómputo (servidores, estaciones de trabajo) deben tener deshabilitados o bloqueados los puertos físicos: USB, puertos seriales, paralelos, inalámbricos (infrarrojos, bluetooh y WAP).

   Se exceptúan los equipos de cómputos (servidores, estaciones de trabajo) que para su operación básica de iniciación, configuración o cargue de software lo requieran. En estos casos se debe tener la justificación de la oficina de sistemas, así mismo, una vez realizada esta operación se debe proceder a deshabilitar el puerto

2. La utilización de dispositivos de almacenamientos removibles en los equipos de cómputos del hospital o de terceros al servicio de este no está autorizada.

3. Las excepciones a los numerales anteriores son autorizadas por la oficina de sistemas.

4. Los casos especiales para los cuales se requiere el uso de estos dispositivos, deben ser evaluada y autorizada por la oficina de sistemas; la justificación debe estar basada en que en que las labores propias del cargo lo hacen indispensable, como por ejemplo copias en CD de firmas digitales, copia de CD para envió de software.

5. En cualquier de los dos casos anteriores se debe cumplir con las siguientes disposiciones:

   - Previo a su utilización, todo dispositivo de almacenamiento removible, debe ser revisado a través de las herramientas de verificación de código malicioso (antivirus), entre otros.

   - La información puede ser almacenada en medios removibles solo cuando sea necesario para el desempeño de las funciones asignadas o cuando la información sea requerida por entes externos.

   - Si la información a copiar en el dispositivo de almacenamiento removibles es confidencial, esta deberá estar cifrada en todo caso.

     Estas políticas aplican a todo el ámbito del hospital, a sus recursos y totalidad de los procesos, ya sean internos o externos, siendo de estricto cumplimiento por todos y cada uno de los funcionarios vinculados directamente mediante contrato a término indefinido, fijo o temporal.

5.4.5 Otros

TRD. 322.1.28.126

1. Los equipos portátiles de computación (laptop, notebook, palm, entre otros) se deben llevarse como equipaje de mano en los viajes y no perderse de vista cuando se encuentre en áreas públicas.

2. Todo equipo portátil debe tener declaración de responsabilidad, la cual incluya instrucciones de manejo de información (encriptación de información confidencial). El acato de normas internas (realización de respaldo periódicos y porte de carne para ingreso y salida de edificios) y seguridad (llevarse como equipaje de mano) para evitar el robo o pérdida.

5.5. Política de software – administración, operación, actualización y control del software institucional

Se relaciona a continuación las políticas que los funcionarios del hospital con funciones y responsabilidades para con el software institucional deben seguir para la correcta administración y protección de este activo y de la información que atreves de él se maneja.

5.5.1. Derechos de autor

1. Todos los derechos de propiedad patrimonial del software desarrollado o modificado por los funcionarios del hospital, durante el tiempo que dure su relación laboral son propiedad exclusiva de la institución.

2. La documentación y el software de propiedad del hospital incluirán avisos sobre derechos de autor y propiedad intelectual.

3. Se debe establecer una adecuada administración de las licencias de software instalado en el hospital que garantice el cumplimiento de las normas legales sobre propiedad intelectual y derechos de autor y la consistencia entre la cantidad adquirida y la instalada.

4. Cuando un tercero administre, desarrolle, pruebe, opere o actualice software del hospital, el tercero debe firmar un acuerdo de confidencialidad en relación con la información a la que tenga acceso.

5.5.2. Control del software

1. El licenciamiento y custodia de software (medios físicos) es responsabilidad de la oficina de sistemas en lo relacionado a software básico y de seguridad informática.

TRD. 322.1.28.126

2. La administración y custodia de las fuentes y versiones del software que esta e desarrollo interno o contratado es responsabilidad de la oficina de sistemas.

5.5.3. Administración del software

El hospital cuenta con software que permite prestar los servicios y manejar la información en condiciones de calidad y seguridad.

1. El uso de software debe cumplir con los estándares de tecnología definidos y autorizados por la oficina de sistemas.

2. El software utilizado por el hospital para prestar sus servicios debe contar con soporte del fabricante o proveedor y previa autorización de la oficina de sistemas

3. Los ambientes de desarrollo, prueba, y producción de sistemas misionales y prioritarios deben permanecer separados para su adecuada administración, operación, control y seguridad, sin que el desempeño y la seguridad de un ambiente influya en los demás.

4. La oficina de sistemas utiliza una metodología formal para catalogación del software y control de versiones que influya las áreas responsables de realizar los procesos.

5. El hospital debe contar en todo momento con un inventario actualizado del software de su propiedad (el comprado a terceros, el desarrollado internamente, el adquirido bajo licenciamiento), así como el entregado y el recibido en comodato.

6. Todo el software se clasificará en una de las siguientes categorías: Misión crítica, prioritaria y requerida. El de misión crítica y prioritaria debe tener como mínimo una copia actualizada con su respectiva documentación técnica en un sitio alterno y seguro de custodia

7. Las instalaciones y actualizaciones de los programas en ambiente de producción del hospital, serán realizadas únicamente por personas autorizadas, de acuerdo con los procedimientos internos establecidos.

8. La oficina de sistemas realizara monitoreo periódico al software instalado en el hospital para detectar la instalación de programas no autorizados.

5.5.4. Adquisición del software

1. Los contratos de adquisición de software debe incluir cláusulas para la protección de la confidencialidad de la información.

2. Para la adquisición de software se debe contar con la autorización de la oficina de sistemas y de su participación en caso de ser necesaria.

3. El desarrollo de software al interior del hospital y el comprado a tercero deberá incluir plan de cuentas, plan de auditoría y control de puertas traseras. En el documento de especificaciones para la adquisición de software se debe describir que elementos de los tres mencionados se requieren.

4. Cuando se adquiera una licencia de uso de software o se contrate su desarrollo través de un proveedor nacional, se debe exigir que el vendedor deposite en custodia en una empresa especializada, una copia del software adquirido (fuente u objeto), la documentación técnica respectiva y sus correspondientes actualizaciones. Lo anterior debe ir acompañado de una autorización por escrito del vendedor para que el hospital pueda retirar, cuando por motivos de fuerza mayor el vendedor deje de existir en el mercado o cuando se requerido por un ente legal

5.5.5. Desarrollo del software

1. El hospital debe utilizar una metodología formal para el desarrollo de software que incluya requerimiento o especificaciones, estudio de factibilidad (técnico y económico), diseño (de programas y de datos) y desarrollo. Esta metodología debe incluir los documentos soporte de cada uno de los procesos realizados, sus respectivas autorizaciones, la documentación técnica requerida y los estándares de desarrollo y documentación.

2. Para todo desarrollo de software se debe utilizar herramientas autorizadas por la oficina de sistemas

3. El uso de herramientas de desarrollo está limitado a la oficina de sistemas. Cualquier excepción es evaluada y autorizada por la oficina de sistemas.

4. Los desarrollos de software deben incluir afinamiento de sentencias (SQL, java, Otros) tanto del sistema en línea como procesos Bath, para minimizar los tiempos de respuesta y optimizar el consumo de recursos del sistema, lo cual redunda en mayor oportunidad en el servicio.

5.5.6. Prueba del software

El hospital cuenta con una metodología de pruebas y certificación de software que incluye: conjunto de casos de prueba, la preparación del ambiente, tipos de prueba (funcionales de seguridad y técnicas, entre otras) a realizar según la complejidad del software, la documentación soporte que se debe generar y el proceso de certificación de las mismas.

1. El área de desarrollo de sistemas debe entregar el código fuente del software desarrollado y el programa ejecutable al área de calidad, con el fin de que se pueda comparar la versión anterior y la modificada y se verifiquen los cambios realizados de acuerdo a los requerimientos. Adicionalmente se debe revisar la no existencia de

códigos mal intencionado y debilidades de seguridad, utilizando preferiblemente herramientas automáticas.

2. Cuando se requieran las claves de producción para ejecutar pruebas, su inserción y mantenimiento se debe hacer en forma segura, de acuerdo al procedimiento definidos por el hospital.

3. Cuando, para el desarrollo de las pruebas del software se requiera tomar copias de la información de los pacientes y en especial información confidencial, la misma debe ser destruida una vez concluyan las pruebas.

5.5.7. Instalación del software

El hospital cuenta con procedimientos y controles para el paso de software a producción. El software en operación deberá estar catalogado.

1. Se prohíbe la instalación de software no autorizado por la oficina de sistemas. Ningún funcionario puede instalar software no autorizado.

2. Los terceros (clientes o compañías comerciales) a los cuales se les instale o entregue el software desarrollado por el hospital deberán firmar previamente un acuerdo de licenciamiento y uso que declare que ellos no desensamblaran, modificaran, ni usaran indebidamente estos programas.

5.5.8. Parametrización

El administrador funcional es el encargado de administrar los parámetros de cada sistema y debe tener una bitácora donde se incluyan todos los cambios o modificaciones realizadas a estos.

5.5.9. Mantenimiento del software

1. La oficina de sistemas es el área autorizada para atender requerimiento y servicios relacionados con hardware y software, realizando la solicitud respectiva mediante los canales establecidos.

2. El hospital debe contar con un procedimiento de control de cambios o funcionales que garantice que solo se realicen las modificaciones autorizadas.

3. La documentación de los cambios hechos al software se realizará simultáneamente con el proceso de cambios.

Para soluciones en producción

4. Para ejecución de procesos de mantenimiento a sistemas de información, se deben definir ventanas de tiempo en periodos de baja transaccionabilidad.

5. Es responsabilidad de la oficina de sistemas controlar operativamente los procesos de mantenimiento a los sistemas de información, validando los cumplimientos de parámetros que minimicen los impactos sobre las áreas críticas.

5.5.10. Soporte de software aplicativo

En los casos en que sea requerido el hospital celebrara contratos de soporte con el fabricante o proveedor de los sistemas informáticos empleados con el fin de garantizar la prestación de servicios.

5.6. Política de datos

Se relacionan a continuación las políticas que los funcionarios del hospital con funciones y responsabilidades para con el manejo de información institucional deben seguir para la correcta administración y protección de la misma para evitar pérdidas, accesos no autorizados y utilización indebida de la misma.

5.6.1. Información confidencial

Para todos los efectos, el hospital considera información confidencial aquella en que el nombre, número de identificación y dirección del paciente este acompañada de los datos de la historia clínica

5.6.2. Almacenamiento de información

5.6.2.1. Almacenamiento masivo y respaldo de información

1. Todos los medios magnéticos utilizados para almacenar información por periodos superiores a seis (6) meses, deben estar protegidos para evitar se degradación o deterioro.

2. Los respaldos de la información debe tener un proceso periódico de validación con el fin de garantizar que no ha sufrido ningún deterioro y que se podrá utilizar en el momento en que se necesite.

3. Las estrategias de respaldo (backups) deben ser diseñadas utilizando métodos que garantice la disponibilidad del servicio.

4. La información del hospital debe ser conservada de acuerdo con las normas de la ley vigente y con la vida útil de los productos.

5. La eliminación de la información debe seguir procedimientos seguros y debidamente aprobados por los responsables de la oficina de sistemas y el dueño de la información.

6. La información enviada o recibida a través de correos electrónicos se debe conservar por lo menos un año. Para los casos en que la información sea objeto o soporte de

reclamaciones, quejas, o cualquier proceso de tipo judicial, debe conservarse hasta el momento en que sea resuelto.

7. Los backups de los sistemas de información y redes deben ser almacenados en zonas diferentes a donde reside la información original. Debe haber una persona responsable de su administración y control y se debe contar con un inventario actualizado de los backups existente.

8. Se debe contar con procedimientos estándares para rotulación de medios de almacenamientos magnéticos.

9. Se prohíbe el almacenamiento de información en dispositivos removibles diferentes a los administradores, lo anterior, con el objeto de salvaguardar la confidencialidad, integridad y disponibilidad de la información, evitando pérdidas, accesos no autorizados y utilización indebida de la misma.

5.6.2.2. Utilización de papel reciclaje

1. Toda área que por la naturaleza de sus procesos, genere o manipule información de pacientes, cuya finalidad no sea el archivo de la misma de acuerdo a las normas legales establecidas para cada proceso, debe garantizar que la información sea destruida.

2. Cualquier listado que contenga información de clientes y/o información confidencial no puede ser reutilizada, es decir, listados cuya información se refiera a nombres, dirección, patologías, entre otros

5.6.3. Administración de la información

1. La información del hospital no debe ser vendida, transferida o intercambiada con terceros para ningún propósito diferente al del negocio, en caso de ser necesario lo anterior, se debe autorizar por escrito por el área responsable.

2. Los datos del hospital deben ser modificado únicamente por el personal autorizado de acuerdo con los procedimientos establecidos. De igual forma, el acceso a información confidencial y a las bodegas de información debe restringirse a personal autorizado.

3. Se deben establecer controles para prevenir que funcionarios, contratistas o consultores se lleven información cuando dejen de prestar sus servicios al hospital.

4. Todos los medios de almacenamientos utilizados en el proceso de construcción, asignación, distribución o cifrado de claves deben contar con un proceso de borrado de información realizando la eliminación de información reescribiendo en el medio de

almacenamiento, con ceros binarios un mínimo de tres veces o la destrucción del medio que la contiene mediante incineración o trituración, inmediata después de ser usada.

5. La información histórica almacenada debe contar con los medios, proceso y programas capaces de manipularla sin inconvenientes, teniendo en cuenta la reestructuración que sufren las aplicaciones y los datos a través del tiempo.

6. La utilización de dispositivos de almacenamiento removibles no es permitida, los casos especiales donde se requiera el uso de estos dispositivos, deben ser evaluados y autorizados por la oficina de sistemas.

5.7. Política de seguridad de sistemas información y sistemas operativos – controles de seguridad para cualquier sistema

Los sistemas de información y sistemas operativos del hospital deben contemplar los aspectos mencionados a continuación y los funcionarios deben velar su cumplimiento.

5.7.1. Control de acceso

5.7.1.1. Generales

1. Todos los sistemas automatizados deben utilizar estándares para el nombre de sistemas de información, nombres de programas y archivos tanto en ambiente de producción como en desarrollo, así como en otras convenciones utilizadas en tecnología.

2. El hospital debe establecer una metodología para la definición de usuarios, roles y perfiles

3. El control de acceso a todos los sistemas de cómputo debe realizarse por medio de códigos de identificación y palabras claves únicas para cada usuario.

4. Si el sistema de control de acceso a un computador o red no está funcionando apropiadamente debe suspenderse el acceso a todos los usuarios.

5. Las palabras claves se deben almacenar cifradas cuando estén en medio magnético y en caja fuerte cuando estén registrada en documentos físicos, así mismo no deben ser incorporadas en los programas de software. Los computadores y sistemas de comunicación deben tener implementados controles que impida la recuperación de las palabras claves almacenada.

6. Las claves de acceso a sistemas operativos, bases de datos y equipos de misión crítica debe ser custodiadas en un ambiente seguro para atender situaciones de contingencia.

7. Ningún funcionario debe construir o utilizar mecanismo para identificar contraseñas o código de usuario sin la autorización de la oficina de sistemas.

8. Todas las palabras claves inicialmente emitidas deben ser validadas solamente para la primera conexión del usuario, momento en el cual debe ser cambiada.

9. Los códigos de usuario y claves de acceso son personales e intransferibles.

10. Se debe realizar un control periódico de usuarios (administradores, superusuarios, de emergencia, anónimos, vacantes, invitados, proveedores y temporales) con el propósito de mantener activos solo los vigentes.

11. Las contraseñas de los usuarios administradores de los servidores y de las base de datos deben estar bajo custodia en la oficina de sistemas.

5.7.1.2. Perfiles y privilegios

1. Todo sistema debe tener definido los perfiles de usuario de acuerdo con la función y cargo de los empleados que acceden al sistema, de tal forma que la información solo sea accesible por los usuarios autorizados y en los horarios establecidos.

2. La modificación a los privilegios o perfiles de usuarios deben ser realizadas por usuarios administradores previa autorización del responsable de la aplicación o de la información.

3. El hospital debe contar con normas y procedimiento para la administración de usuarios y perfiles en donde se deje evidencia de los cambios realizados a los perfiles, el estado y la eliminación de las cuentas.

4. Los privilegios especiales del sistema deben otorgarse únicamente a los funcionarios administradores de este o responsables de la seguridad. Los usuarios finales no deben tener acceso a los niveles de comandos para el funcionamiento del sistema ni a programas editores de la información.

TRD. 322.1.28.126

5. Los administradores de los sistemas o superusuarios deben tener por lo menos dos usuarios. Uno de acceso privilegiado (superusuario) y el otro con el que se lleva acabo trabajo diarios.

6. El nivel de superusuario de los sistemas deben tener un control dual, de tal forma que exista una supervisión a las actividades realizadas por el administrador del sistema.

7. Los usuarios de las tareas de desarrollo y prueba de software no debe tener acceso a los ambientes de producción. Por lo tanto los administradores de sistemas para los ambientes de producción, deben ser independiente a los administradores de los ambientes de desarrollo y pruebas

8. Las herramientas de los sistemas de información del hospital que potencialmente puedan causar un daño, deben ser restringidas para que sean solamente usadas en los propósitos determinados.

9. El hardware y software de diagnóstico, monitoreo y/o utilitarios debe ser usados por el personal autorizado.

5.7.1.3. Controles automáticos y de usuarios

5.7.1.3.1.1. Si el usuario digital un nombre de usuario o clave incorrecta, el sistema no debe mostrar la fuente del problema, simplemente informar que el acceso fue negado y solicitar nuevamente los datos.

5.7.1.3.1.2. Después de tres intentos consecutivos fallidos de ingresos al sistema, se debe bloquear el acceso del usuario, el desbloqueo debe ser autorizado por el administrador (funcional, técnico u operativo) y/o responsable de la información

5.7.1.3.1.3. Las palabras claves deben tener la siguiente estructura: longitud minina de 8 caracteres, de los cuales al menos un carácter alfabético en minúscula, otro en mayúscula, un carácter numérico y otro no alfanumérico

5.7.1.3.1.4. Los usuarios deben definir palabras claves que sean difícil de adivinar, no puede ser series de números (12345678), ni repeticiones de caracteres (AAAA, 1111), ni situaciones familiares (fechas de cumpleaños, nombres familiares, placas de vehículos, entre otros), ni palabras compuestas combinadas concierto número de caracteres que cambian predeciblemente (un área, una fecha, una ciudad, un proyecto, entre otros), ni palabras muy similares a otras definidas anteriormente.

TRD. 322.1.28.126

5.7.1.3.1.5. En aquellos sistemas en los que se puede implantar, se debe llevar un histórico de contraseña, mínimo 5, de tal forma que los usuarios no usen las claves utilizadas anteriormente.

5.7.1.3.1.6. Las contraseñas no deben presentar en pantalla, impresoras, ni por ningún medio.

5.7.1.3.1.7. El sistema debe obligar automáticamente a que todos los usuarios cambien sus palabras claves al menos una vez cada 30 días

5.7.1.3.1.8. Al momento de ingreso al sistema, se debe dar a cada usuario la información indicando la última hora y fecha del último acceso. Esto permitirá detectar fácilmente el uso no autorizado al sistema.

5.7.1.3.1.9. El sistema no debe permitir que ningún usuario maneje simultáneamente sesiones múltiples en línea, a menos que se tenga un permiso especial concedido por la oficina de sistemas.

5.7.1.3.1.10. El sistema debe controlar el tiempo de inactividad del usuario y desactivar las sesiones automáticamente después de 5 minutos.

5.7.1.3.1.11. Los usuarios no deben abandonar su estación de trabajo si haber cerrado la sesión.

5.7.1.3.1.12. A todos los usuarios se les debe revocar los privilegios automáticamente cuando no han tenido actividad durante un periodo de quince (15) días.

5.7.1.3.1.13. Si se utiliza palabras claves generadas por el sistema, estas se deben construir de forma aleatoria.

5.7.1.3.1.14. En el evento que un usuario se encuentre bloqueado y no recuerde su contraseña, requiere para su desbloqueo el visto bueno del jefe inmediato. Se exceptúa de esta política el primer, segundo y tercer nivel dela organización.

5.7.2. Logs

5.7.2.1.1.1. Todos los sistemas de información que operen y administren información confidencial del hospital como son los sistemas de información, sistemas operativos, sistemas de base de datos y telecomunicaciones deben generar logs de auditoria.

5.7.2.1.1.2. Todos los archivos de log deben proporcionar suficiente información para apoyar el monitoreo, control y auditoria. El hospital se reserva el derecho de revisión de los mismos.

5.7.2.1.1.3. Los log de consulta de información confidencial de los pacientes debe incluir como mínimo la siguiente información:

- Identificación del funcionario que la realizo.
- Identificación del sistema de información.
- Identificación del equipo.
- Fecha y hora de la consulta.
- Número de identificación del paciente consultado

5.7.2.1.1.4. Todos los archivos de log de los diferentes sistemas de información deben retenerse por periodos definidos según su criticidad y la exigida de ley en forma obligatoria. Además, deben ser custodiada en forma segura para que no puedan ser modificados y para que puedan ser leídos únicamente por personal autorizado.

5.7.2.1.1.5. Los log son evidencia digital suficiente y competente de la utilización de los aplicativos, sistemas operacionales y comunicaciones y puede ser utilizada por el hospital en todos los casos que consideren necesarios (investigaciones internas, investigaciones externas, consultas de entes externo y entes de control).

5.7.2.1.1.6. Las aplicaciones de misión crítica requieren tener archivos de logs robustos que permitan reanudar las actividades del sistema en un tiempo prudente cuando se presenta una contingencia.

5.7.2.1.1.7. Todos los log habilitados en el sistema debe tener definido un usuario para su administración y control, quien además deberá encargarse de realizar seguimientos y revisión periódica a los mismos.

5.7.2.1.1.8. Todos los computadores del hospital deben sincronizado y tener la fecha y hora exacta de acuerdo con el estándar internacional, para que el registro en los log sea correcto.

5.7.2.1.1.9. Los log deben contar con mecanismo de seguridad y control administrativo que permitan detectar y resistir ataques, y grabar estos eventos; estos ataques incluyen intentos de desactivar, modificar o detectar las claves de acceso al software y/o a los mismos logs. El acceso a los logs está restringido únicamente al personal autorizado y que lo requiera para el desarrollo de sus funciones.

TRD. 322.1.28.126

5.7.3. Otros controles

5.7.3.1.1.1. Todo sistema debe contener herramientas que ayuden al administrador a la verificación del estado de seguridad de los sistemas. Estas herramientas deben contener mecanismo que sirvan para detectar, informar y corregir problemas de seguridad.

El hospital utiliza software antivirus residente en los computadores o estaciones de trabajo para proteger la información residente e ellos, además debe procurar su actualización periódica; igualmente el software utilizado debe controlar y restringir el ingreso de correo spam.

5.7.3.1.1.2. Los sistemas de información en producción debe ser evaluados periódicamente por las áreas de control del hospital para determinar el cumplimiento de un conjunto mínimo de controles requeridos para reducir el riesgo a un nivel aceptable.

5.7.3.1.1.3. Los discos duros y otros medios de almacenamiento en línea usados en sistemas en producción no deben contener compiladores, ensambladores, editores de texto, procesadores de palabras u otras utilidades de propósito general que puedan usarse para comprometer la seguridad de las misma.

5.7.3.1.1.4. Las funcionalidades del software que son innecesarias en el ambiente informativo del hospital se deben desactivar en el momento de su instalación.

5.7.3.1.1.5. Se deben establecer procedimientos de monitoreo para detectar instalaciones de hardware o software no autorizado.

5.7.3.1.1.6. Los sistemas operacionales de los equipos empleados en las oficinas deben cumplir con el nivel de seguridad de protección de acceso controlado.

5.7.4. Definición de protocolos, servicios, aplicaciones, usuarios a tener en operaciones

5.7.4.1.1.1. Dentro de las operaciones normales del hospital se debe identificar todos aquellos protocolos, servicios, puertos, aplicaciones y usuarios involucrados en los sistemas de cómputo.

TRD. 322.1.28.126

5.7.4.1.1.2. Asi mismo, se debe identificar todos aquellos protocolos, servicios, puertos, aplicaciones y usuarios que no se consideren necesarios y que puedan representar un riesgo en caso de quedar activos en pleno funcionamiento.

5.7.4.1.1.3. El área de sistemas debe identificar dentro del inventario de servidores y equipos, aquellos servicios, usuario, aplicaciones, puertos y protocolos que se consideran necesarios, útiles o activos para el correcto y seguro funcionamiento de las operaciones generales en la organización, considerando los siguientes aspectos:

- Efectuar de manera periódica, cada seis (6) una revisión de puertos de comunicación, protocolos, servicios, aplicaciones y en general todo aquello que represente un riesgo de seguridad o una carga operativa para identificar aquellos que no generen utilidad o beneficio.
- Bloquear o suspender aquellos servicios que en general representen una amenaza de seguridad detectada en el análisis llevado a cabo.

5.8. Política de instalación física

Se relaciona a continuación las políticas de seguridad física que los funcionarios deben seguir con el fin de salvaguardar los recursos técnicos e informáticos del hospital.

5.8.1. Control de acceso físico

El hospital debe contar con los mecanismos de control de acceso tales como puertas de seguridad, sistemas de control con tarjetas inteligentes y sistemas de alarma, en las dependencias en que el hospital considere crítica.

5.8.1.1. Personas

5.8.1.1.1.1. Los visitantes como los empleados deben portar un dispositivo o escarapela visible que los identifique. Adicionalmente cuando requieran ingresar a áreas críticas deben hacerlo en compañía de un funcionario de dicha área.

5.8.1.1.1.2. Tanto visitantes como los empleados deben tener acceso únicamente a las áreas, información y recursos necesarios para el desarrollo de sus actividades.

TRD. 322.1.28.126

5.8.1.1.1.3. Los códigos de acceso de los funcionarios que dejen de tener vínculos laborales con el hospital deben ser cambiados o desactivados, en forma oportuna.

5.8.1.1.1.4. En caso de pérdida de escarapelas o tarjetas de acceso se debe informar inmediatamente a la persona responsable para su desactivación.

5.8.1.1.1.5. Se debe mantener por un periodo de un (1) año el registro de acceso del personal autorizado y de ingreso, con el objeto de facilitar proceso de seguimiento.

5.8.1.1.1.6. No se deben ingerir alimentos, fumar, o beber en el centro de cómputo o instalaciones con equipos de computación

5.8.1.1.1.7. Todos los sistemas de control de acceso deben ser monitoreados permanentemente.

5.8.1.2. Equipos y otros recursos

5.8.1.2.1.1. Toda sede y equipo informático ya sea propio o de tercero, en donde se procese información del hospital o posean un vínculo especial con la misma, debe cumplir con todas las normas de seguridad física emitida, con el fin de evitar el acceso a personas no autorizadas

5.8.1.2.1.2. Los equipos de propiedad del hospital como equipos portátiles, equipos de cómputos, máquinas de escribir, entre otros, no deben moverse, reubicarse o retirarse de las instalaciones físicas sin autorización de las ares responsables.

5.8.1.2.1.3. Todo maletín, caja o bolso debe ser revisado por el personal de seguridad tanto al momento de acceder a las instalaciones como al momento de salir de ellas.

5.8.1.2.1.4. No se debe proveer información sobre los sistemas de control de acceso, seguridad física e información, así como dela ubicación de las áreas donde se procesa información

5.8.2. Protección física de la información

Todas las personas que laboren para el hospital y/o aquellas designadas para trabajar en actividades particulares (consultores y contratistas) son responsables del adecuado uso de la información suministrada para tal fin.

5.8.3. Protección contra desastres

TRD. 322.1.28.126

Los equipos procesamiento y comunicaciones deben encontrarse localizadas en áreas seguras que cuenten con medidas para prevenir inundaciones, robos, interferencias electromagnéticas, fuego, humo y demás amenazas que puedan interferir con su buen uso y la continuidad del servicio.

5.9. Política de seguridad en redes de comunicación

5.9.1. Ambiente

Se relaciona a continuación las políticas que el área de sistemas (Administrador de las redes de comunicaciones) debe seguir para proteger la información que por ella fluya.

5.9.1.1. Aspectos Generales

5.9.1.1.1.1. La información confidencial que viaje por las redes de comunicaciones propias y externas debe estar cifrada.

5.9.1.1.1.2. Las direcciones internas, configuraciones e información de comunicación y cómputo del hospital debe ser tratadas como información confidencial.

5.9.1.1.1.3. Los empleados y contratistas no deben llevar a cabo ningún tipo de instalación de líneas telefónicas, canales de transmisión de datos, módems, router, ni cambiar su configuración sin haber sido formalmente aprobados por la oficina de sistemas.

5.9.1.1.1.4. El hospital debe establecer fuertes mecanismos de seguridad física en las centrales de conexión o centros de cableados.

5.9.1.1.1.5. Los empleados o contratistas no deben llevar a cabo ningún tipo de grabaciones o captura en los canales de transmisión de datos, deben instalarse previa aprobación formal de las áreas responsables del hospital, además todo software que permita realizar monitoreo (sniffers y analizadores de protocolos) sobre estos canales debe estar debidamente aprobado.

5.9.1.2. Conexiones con redes públicas e Internet

Toda conexión entre las redes las redes del hospital y redes externas de servicios, redes públicas e internet debe contar como mínimo con mecanismos de control de acceso lógico, tales como: firewall, proxys, entre otros; igualmente todos los usuarios deben autenticarse ante estos mecanismos de seguridad.

5.9.1.3. Conexiones a redes amplias, redes metropolitanas y locales

TRD. 322.1.28.126

El hospital debe proponer por segmentar las redes de comunicaciones de tal forma que los usuarios mantengan una independencia sobre las mismas.

5.9.1.4. Outsourcing

5.9.1.4.1.1. Las conexiones entre sistemas internos del hospital y otros de terceros es aprobado y certificada por la oficina de sistemas con el fin de no comprometer la seguridad de la información del hospital.

5.9.1.4.1.2. Los equipos de computación del hospital que sean accedidos por terceros a través de diversos canales deben ser protegidos por mecanismos de control aprobados por la oficina de sistemas

5.9.1.4.1.3. En la selección de proveedores de comunicación se debe tener en cuenta compañías debidamente establecidas, con licencias de operación y una amplia trayectoria en el mercado.

5.9.1.4.1.4. Las desconexiones de equipos de seguridad instalados para el monitoreo y control de las comunicaciones, debe ser autorizada por la oficina de sistema.

5.9.1.4.1.5. Se prohíbe el ingreso y utilización de dispositivos que permitan almacenar o copiar información, o medios de comunicación que no sean suministrados por la entidad

5.9.1.5. Acceso remoto

5.9.1.5.1.1. El hospital no tiene la obligación de otorgar servicio de ingreso a internet a los funcionarios desde sitios diferentes a su lugar de trabajo, excepto a aquellos con los cuales se ha convenido para el desarrollo de sus actividades laborales. Los usuarios que ingresen en la red se hacen responsables por los daños que ocasionen en forma no autorizada.

5.9.1.5.1.2. Las conexiones con los sistemas y redes del hospital deben ser dirigidas a través de dispositivos probados y aprobados por la oficina de sistemas.

5.9.1.5.1.3. Los equipos de cómputos del hospital que se acceden por terceros a través de diversos canales, deben ser protegidos por mecanismos de control aprobados por la oficina de sistemas.

5.10. Políticas de seguridad en la utilización del correo electrónico

TRD. 322.1.28.126

5.10.1.1.1.1. El sistema de correo electrónico del hospital debe ser usado fundamentalmente para propósitos de trabajos.

5.10.1.1.1.2. Ningún empleado está autorizado para monitorear los mensajes de correo electrónicos.

5.10.1.1.1.3. El hospital debe establecer normas para proteger la confidencialidad, privacidad e integridad de la información (disclaimers/notas/observaciones) obtenida a través de sus servicios de correo electrónico, teniendo en cuenta los siguientes parámetros: tipo de información que se obtiene, finalidad que se dará a la información, modificación o actualización de la información, aceptación de los términos por las partes involucradas.

5.10.1.1.1.4. Los archivos y mensajes de correo son información privada. El correo electrónico se debe manejar como comunicación directa y privada entre el organizador y el receptor. Los funcionarios no deben utilizar una cuenta de correo electrónico que pertenezca a otro funcionario. Si hay necesidad de hacerlo en caso de ausencia o vacaciones se debe recurrir a mecanismos alternos como redirección de mensajes. Todo mensaje dirigido a terceros (personas que no hacen parte de la institución) a través del sistema de correo electrónico, es confidencial y privado represente o no la disposición de la entidad, por ello se debe incluir siempre al final del mensaje el disclaimers que adopto la entidad para todos los correos salientes, así:

Las opiniones contenidas en este mensaje son las de su autor y no corresponde necesariamente a las institucionales de la entidad, salvo que en su razón de su cargo el autor este facultado para expresarlas. Toda información contenida en este mensaje es considerada de carácter confidencial y/o privilegiado y está dirigida únicamente a su destinatario, quien por tal razón es el único autorizado para leerla y utilizarla. Si usted ha recibido por error este mensaje debe eliminarlo totalmente de su sistema y comunicar tal situación al remitente de inmediato. El receptor deberá verificar posibles virus informáticos que este mensaje o sus anexos puedan tener. La institución no se hace responsable por los daños que tales virus puedan causar.

5.10.1.1.1.5. El correo electrónico no debe ser utilizado por terceros sin previa autorización de la oficina de sistemas.

TRD. 322.1.28.126

5.10.1.1.1.6. El envió de mensajes masivos at raves de correos electrónicos debe ser realizado solo por las áreas previamente autorizadas por la oficina de sistemas.

5.10.1.1.1.7. Los empleados no deben enviar mensajes de correo electrónico con contenidos hostiles que molesten a los receptores del mismo, tales como comentarios sobre sexo, raza, religión, o preferencias sexuales; así mismo, cuando un empleado reciba este tipo de mensajes debe comunicarlo a su jefe inmediato.

5.10.1.1.1.8. Los funcionarios no puede utilizar versiones digitales de firmas hechas a mano para dar impresión de que un mensaje de correo electrónico o cualquier otro tipo de comunicación electrónica haya sido firmada por la persona que la envía.

5.10.1.1.1.9. Los funcionarios no deben abrir los mensajes anónimos o desconocidos. Por el contrario, deben borrarlos sin leerlos. Asi mismo, no deben ejecutar archivos anexados en mensajes de correos de fuente externa del hospital y no deben deshabilitar el antivirus instalado en su computador. Por esta causa todo mensaje tiene que tener declarada la referencia o asunto en el reglón correspondiente.

5.10.1.1.1.10. Es prerrequisito que los equipos tengan instalado, configurado y actualizado el antivirus para poder hacer uso del correo electrónico; igualmente el software utilizado debe controlar y restringir el ingreso de correo spam.

5.10.1.1.1.11. La clave de ingreso de las estaciones no se comparte. Cada funcionario es responsable por los mensajes que son enviados desde su estación y con su cuenta de usuario de correo electrónico.

5.10.1.1.1.12. La responsabilidad de leer a diario el correo es de todos los y su desatención no es excusa para no darse por enterado de los mensaje que llegan.

5.10.1.1.1.13. La información enviada por intermedio del correo electrónico es tan válida y consistente como lo que habitualmente se emite por otros medios de comunicación. Por lo tanto su acatamiento y manejo debe obedecer a las mismas normas con las cuales se maneja las comunicaciones al interior del hospital.

5.10.1.1.1.14. No envie ni sea parte de una cadena de mensajes. Estos es considerado como falta grave y puede acarrear sanciones dentro del hospital aunque no haya sido usted la persona que comenzó con la

TRD. 322.1.28.126

cadena. En caso de recibir un mensaje de este tipo, debe reenviarse al correo de la oficina de sistemas.

5.10.1.1.1.15. Esta prohibido suscribirse a lista de distribución de amigos, grupos, mercadeo, publicidad, ventas, entre otros, por internet.

5.10.1.1.1.16. El correo es privado e individual.

5.10.1.1.1.17. El correo electrónico no puede reemplazar los canales oficiales establecidos por el hospital para el envió de la información (reclamo, documentos que deben ser enviados en medio físico, entre otros).

5.10.1.1.1.18. Debe evitarse imprimir mensajes de correo. Si se requiere una copia para archivo, puede hacerse en medio magnético o en el disco duro del computador. Es importante que en la red no se deje estos archivos pues limitan el espacio destinado para este fin.

5.10.1.1.1.19. Los usuarios no deben habilitar la funcionalidad que deja reconocer la vista previa de cada uno de los correos, lo anterior debido a que permite la activación y propagación de virus y software malicioso.

5.11. Política de seguridad en la utilización de internet

Se relaciona a continuación las políticas que los funcionarios del hospital a quienes se les haya asignado el servicio de internet deben seguir para proteger la información ante los riesgos de pérdida de confidencialidad, integridad y disponibilidad a través del uso de internet.

Igualmente, instruir a todos los funcionarios del hospital en la utilización del servicio de internet, generándose un ambiente de seguridad de la informacion, con el propósito de que su manipulación no se convierta en una debilidad ante la presencia de software que pueda dañarla.

5.11.1. Autorización del servicio

5.11.1.1.1.1. Se asigna el servicio de internet (navegación y/o correo electrónico), únicamente a aquellos funcionarios que lo requieran por el desempeño de sus funciones, previa aprobación del jefe inmediato.

5.11.1.1.1.2. El hospital se reserva el derecho de hacer seguimiento, para lo cual realizara pruebas de auditoria detallada de los logs correspondiente.

5.11.2. Uso del servicio

TRD. 322.1.28.126

5.11.2.1.1.1. Se restringe el uso de correos masivos que puedan afectar el buen funcionamiento del servicio de internet. Estos deben ser dirigidos de manera individual y con copia a los interesados, pero no a grupos extensos.

5.11.2.1.1.2. En cualquier momento en que un trabajador publique mensajes en grupos de discusión de internet en un boletín electrónico, o cualquier otro sistema de información público, este mensaje debe ir acompañado de palabras que indiquen claramente que su contenido no representa la posición del hospital. Dichas frases son requeridas aun cuando el nombre del hospital no aparezca en el texto del mensaje.

5.11.3. Seguridad

5.11.3.1.1.1. Los funcionarios del hospital no deben bajar y cargar software de internet en los sistemas de la entidad a menos que sea necesario para el desempeño de su función y previa autorización de la oficina de sistemas.

5.11.3.1.1.2. Todas las conexiones deben ser realizada a través de la red del hospital. Las no realizadas mediante la red deben ser efectuadas desde computadores aislados dela red con previa aprobación de la oficina de sistemas.

5.11.3.1.1.3. Los archivos bajados de internet deben ser verificados mediante la utilización de un paquete de detección de virus autorizado, antes de ser transmitido a otro computador.

5.11.3.1.1.4. El hospital no tiene la obligación de otorgar servicio a internet a los funcionarios desde sitios diferentes a su lugar de trabajo, excepto a aquellos con cuales se ha convenido para el desarrollo de sus actividades laborales. Los usuarios que ingresen en la red del hospital se hace responsable por los daños que ocasione en forma no autorizada.

5.11.3.1.1.5. Cuando se estén utilizando los servicios de internet del hospital, los funcionarios no deben suplantar caros y/o personas o brindar identificación inexacta.

5.11.3.1.1.6. La oficina de sistemas garantizara que la información publicada en internet cuente con los mecanismo de seguridad informática que eviten su modificación

5.11.3.1.1.7. La información confidencial del hospital no debe quedar residente en intranet y/o internet.

TRD. 322.1.28.126

5.11.4. Otras – conexión

5.11.4.1.1.1. Los funcionarios deben abstenerse de ingresar a páginas de internet que contengan contenidos sexuales, racistas, o cualquier otro tipo de material ofensivo, dado que no aportan a la ejecución de su trabajo.

5.11.4.1.1.2. El hospital se reserva el derecho de restringir el ingreso a páginas que considere no necesarias.

5.11.5. Publicación

5.11.5.1.1.1. Todos los cambios que se hagan en la página web del hospital en internet debe ser aprobados por la oficina de sistemas y/o imagen corporativa.

5.11.5.1.1.2. Los usuarios no deben publicar material del hospital (software, memos internos, publicaciones de prensa, entre otros) en ningún computador que tenga acceso a internet.

5.11.5.1.1.3. La página web del hospital en internet debe ajustarse a estándares de diseño, navegación, redacción legal y requerimiento similares establecidos por la oficina de sistemas y/o imagen corporativa.

5.11.6. Privacidad

En internet aplican las leyes para el derecho de reproducción, patente, marcas registradas, y todo lo relacionado, por lo que los funcionarios que utilicen este servicio deben saber:

- Publicar material únicamente después de obtener permiso de la fuente
- Indicar la fuente únicamente si esta es idéntica
- Revelar información interna del hospital en internet solo si esto ha sido aprobado.

5.11.7. Aspectos técnicos

5.11.7.1.1.1. La conexión directa entre un computador del hospital y otra organización vía redes públicas de datos como internet requieren de la aprobación de la oficina de sistemas, quien estipulara los mecanismos de seguridad apropiados, los cuales deben incluir un firewall y otros mecanismos de control adicionales.

5.11.7.1.1.2. Se definirá conexiones robustas al mundo de internet, las cuales deberán ser controladas y protegidas por la oficina de sistemas.

TRD. 322.1.28.126

CONTROL DE CAMBIOS.

REVISIÓN N°	FECHA DE APROBACIÓN DD/MM/AA	DESCRIPCIÓN DE CAMBIOS
01	13/08/2018	Creación del Documento
	-	