RESUMEN – TRABAJO DE GRADO

AUTORES	**GERARDO CESAR MOSQUERA QUINTERO** **JORGE ARMANDO SARAVIA ALVERNIA** **JOSE JULIAN PACHECO PEREZ**
FACULTAD	**FALCULTAD DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS**
DIRECTOR	**ANDRES MAURICIO PUENTES**
TÍTULO DE LA TESIS	**ELABORACIÓN DE POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2013 EN EL HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE ESE. DE LA CIUDAD DE AGUACHICA-CESAR.**

RESUMEN

(70 palabras aproximadamente)

EL PRESENTE TRABAJO TIENE POR OBJETIVO LA CREACIÓN DE LAS POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL QUE BRINDE APOYO PARA PODER PROTEGER LA INFORMACIÓN EN EL HOSPITAL JOSE DAVID PADILLA VILLAFAÑE DE AGUACHICA, PARA LAS MEJORES PRÁCTICAS EN EL USO ADECUADO SEGÚN LOS LINEAMIENTOS DEL ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2013, Y A SU VEZ PROPORCIONAR UN PLAN DE MEJORA PARA LA OPTIMIZACIÓN, BRINDANDO RECOMENDACIONES EN FORMA SENCILLA Y ENTENDIBLE, ACERCA DE CÓMO MEJORAR LOS PROCESOS PAR A PROTEGER LA IN FORMACIÓN.

CARACTERÍSTICAS

PÁGINAS: 126	PLANOS: 0	ILUSTRACIONES:10	CD-ROM: 1

ELABORACIÓN DE POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2013 EN EL HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE ESE. DE LA CIUDAD DE AGUACHICA-CESAR.

MOSQUERA QUINTERO GERARDO CESAR
PACHECO PÉREZ JOSÉ JULIÁN
SARAVIA ALVERNIA JORGE ARMANDO

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
OCAÑA
2015

ELABORACIÓN DE POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL BASADOS EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2013 EN EL HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE ESE. DE LA CIUDAD DE AGUACHICA-CESAR.

MOSQUERA QUINTERO GERARDO CESAR
PACHECO PÉREZ JOSÉ JULIÁN
SARAVIA ALVERNIA JORGE ARMANDO

Proyecto de grado presentado como requisito parcial para optar el título de Especialista en Auditoria de Sistemas

DIRECTOR
ANDRÉS MAURICIO PUENTES VELÁSQUEZ
IS. ESP. MSC. Ingeniería de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
ESPECIALIZACIÓN EN AUDITORIA DE SISTEMAS
OCAÑA
2015

DEDICATORIA

Dedico este logro principalmente a Dios por darme la sabiduría para alcanzar cada una de las metas y objetivos propuestos.

A mi madre María Aurora Alvernia a mi padre Carlos Jorge Saravia y mi hermana Angie Lorena Martinez Alvernia, a ellos por su apoyo en mis estudios, gracias por permitir de mis sueños una realidad.

A mi hijo Dylan Sebastián Saravia a mí a mi Mujer Cindy Carolina Rojas por ser el motor que día a día me impulsa a seguir adelante.

Y demás familiares y amigos quienes han compartido conmigo en este largo camino y hoy ven este sueño realidad.

JORGE ARMANDO SARAVIA ALVERNIA

AGRADECIMIENTOS

Agradezco a Dios por darme la sabiduría y entendimiento que me permiten alcanzar cada una de mis metas propuestas y hacer realidad este gran sueño.

A los profesores que nos instruyeron en este gran reto que fue la especialización.

A mis compañeros Gerardo Mosquera, Julián Pacheco, a ustedes mil y mil gracias por ser un grupo selecto y comprometido, por su apoyo y entrega en este proyecto.

JORGE ARMANDO SARAVIA ALVERNIA

DEDICATORIA

Dedico este logro principalmente a Dios por darme la sabiduría para alcanzar cada una de las metas y objetivos propuestos.

A mi madre Gloria Esther Pérez Ascanio y mi padre José Luis Pacheco Bautista a ellos por su apoyo en mis estudios, gracias por permitir de mis sueños una realidad y mis hermanos José Fabián, José Luis y Rafael José Pacheco Pérez por apoyarme incondicionalmente y compartir conmigo cada momento de mi vida.

A mi novia Ivian Nurieth Madariaga que es mi motor por su amor, dedicación y comprensión por darme fuerzas e impulsarme para seguir adelante.

Y demás familiares mi Tía Claudia Patricia Pacheco, mi Tío Osman Rafael Jalkh, a mis abuelos Rafael Antonio Álvarez y Fabiola Bautista Pérez, quienes han compartido conmigo en este largo camino y hoy ven este sueño realidad.

JOSE JULIAN PACHECO PEREZ

AGRADECIMIENTOS

Agradezco a Dios por la sabiduría y entendimiento que me permiten alcanzar cada uno de mis objetivos e ideales y hacer realidad este gran sueño.

A mis padres por haberme brindado la oportunidad de optar a la realización de una carrera con esfuerzo y dedicación.

A mis compañeros Gerardo Mosquera, Jorge Saravia, gracias por ser un grupo selecto y comprometido, por su apoyo y entrega en este proyecto que hace unos meses emprendimos y que hoy nos permite el paso una vez más alcanzar una meta.

JOSE JULIAN PACHECO PEREZ

DEDICATORIA

Dedico este trabajo de grado, el cual culmino con mucho esfuerzo y también con mucho amor especialmente a mis padres que aunque no están en el mundo terrenal siento que siempre me acompañan y sé, que donde se encuentren estarán orgullosos de su hijo.
A mi esposa Tania Marcela y a mi hijo Cesar Alejandro, los cuales son el faro que me guía y el motor que me impulsa a seguir adelante.
A mi familia y cada una de las personas que de alguna u otra manera, contribuyeron a que lograra esta meta que me propuse en la vida, y que me ha permitido crecer intelectualmente como persona y como ser humano.

GERARDO CESAR MOSQUERA QUINTERO

AGRADECIMIENTO

A Dios, por darme la vida, la fortaleza, la salud y el amor para seguir siempre adelante sin decaer.
A mis amigos y compañeros de estudio Julián y Jorge en los cuales me apoye para culminar la especialización.
A los profesores que nos instruyeron en este gran reto que fue la especialización.

GERARDO CESAR MOSQUERA QUINTERO

CONTENIDO

Pág.

INTRODUCCIÓN 13

1. TITULO 14
1.1 PLANTEAMIENTO DEL PROBLEMA 14
1.2 FORMULACIÓN DEL PROBLEMA 14
1.3 OBJETIVOS 14
1.3.1 Objetivo General 14
1.3.2 Objetivos Específicos 15
1.5 JUSTIFICACIÓN 15
1.6 HIPÓTESIS 15
1.7 DELIMITACIÓN 16
1.7.1 Temporal 16
1.7.2 Espacial 16
1.7.3 Contextual. 16

2. MARCO REFERENCIAL 18
2.1 MARCO HISTORICO 18
2.2 MARCO CONTEXTUAL 19
2.3 MARCO CONCEPTUAL 19
2.4 MARCO TEÓRICO 21
2.4.1 PLAN ESTRATÉGICO 21
2.4.2 GOBERNABILIDAD DE TI 22
2.4.3 Seguridad Física 24
2.4.4 Amenazas previstas en Seguridad Física 25
2.4.5 Desastre 25
2.4.6 Vulnerabilidad 25
2.4.7 Mitigar 26
2.4.8 Seguridad Física y del Entorno o Ambiente 26
2.5 MARCO LEGAL 28

3. DISEÑO METODOLÓGICO 30
3.1 Tipo de Investigación 30
3.2 Población 30
3.3 Muestra 30
3.4 Instrumentos de recolección de información 31
3.5 Análisis de la información 31
3.6 Tabla de seguimiento metodológico 31

4. PRESENTACIÓN DE RESULTADOS 33

4.1. DESCRIPCIÓN Y CARACTERIZACION DEL HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE. 33
4.1.1 Misión 33
4.1.2 Visión 33
4.1.3 Principios corporativos 33
4.1.4 Valores corporativos 34
4.1.5 Organigrama de la organización 36
4.2 Diagnóstico de la seguridad de la información física y del ambiente del Hospital Regional José David Padilla Villafañe. 37
4.3 EVALUACION DE RIESGOS 40
4.4 Cuadro comparativo de verificación de estado actual del Hospital 43
4.5 POLITICAS DE SEGURIDAD FISICA Y DEL AMBIENTE 46
4.6 PLAN DE MEJORAMIENTO 52
4.7 PRUEBA PILOTO AL OBJETIVO DE CONTROL 11.2.4 MANTENIMIENTO DE LOS EQUIPOS. 53

CONCLUSIONES 76

RECOMENDACIONES 77

BIBLIOGRAFÍA 78

CYBERGRAFIA 80

ANEXOS 81

LISTA DE FIGURAS

Figura 1. Mapa geográfico de Aguachica 16
Figura 2. Formula muestra 30
Figura 3. Organigrama de la Organización 36
Figura 4. Planillas de ejecución mal diligenciadas e incompletas 60
Figura 5. Resolución plan de mantenimiento 61
Figura 6. Divulgación plan de mantenimiento 63
Figura 7. Plantillas de ejecución correctamente diligenciadas 65
Figura 8. Actas de comparación plan de mantenimiento vs plantilla de ejecución. 66
Figura 9. Conocimientos de las fechas de los mantenimientos preventivos de los equipos de cómputo. 73
Figura 10. Conformidad con los mantenimientos realizados 74

TABLAS

Tabla 1. Seguimiento metodológico 31
Tabla 2. Probabilidad 37
Tabla 3. Impacto 37
Tabla 4. Marcador de riesgo para un riesgo especifico 38
Tabla 5. Riesgo 38
Tabla 6. Cuadro de comparación 43
Tabla 7. Plan de mantenimiento de equipos de computo 55
Tabla 8. Conocimientos de las fechas de los mantenimientos preventivos de los equipos de cómputo. 73
Tabla 9. Conformidad con los mantenimientos realizados 74
Tabla 10. Cuadro comparativo encuesta anterior vs encuesta actual 74

INTRODUCCIÓN

En la actualidad siempre ha existido dos elementos importantes que buscan una adecuada seguridad de la información: la importancia creciente de la información para las empresa ya que es considerada como su activo principal de operaciones y el aumento de los riesgos a la que la misma se ve expuesta.

El Hospital Regional José Padilla Villafañe localizado en la ciudad de Aguachica Cesar brinda servicios de salud de segundo nivel de complejidad confiable y segura a la región sur del Cesar y sur del Bolívar, maneja información confidencial y de gran importancia para el desarrollo de actividades.

El presente trabajo tiene por objetivo la creación de las políticas de seguridad física y ambiental que brinden apoyo a la protección de la información en el Hospital José David Padilla Villafañe de Aguachica, para las mejores prácticas en la custodia de la misma, según los lineamientos del estándar internacional ISO/IEC 27002:2013, y a su vez proporcionar un plan de mejora para la optimización, brindando recomendaciones en forma sencilla y entendible, acerca de cómo mejorar los mecanismos para salvaguardar la información.

La metodología utilizada para la elaboración de este proyecto se basó en la aplicación una auditoria previa y basada en el estándar ISO/IEC 27002:2013, en su dominio "11 SEGURIDAD FISICA Y AMBIENTAL", para posteriormente estructurar el análisis de riesgos que nos permitió identificar las debilidades y amenazas presentadas por el Hospital y finalmente desarrollar las políticas.

1. TITULO

Elaboración de políticas de seguridad física y ambiental basados en el Estándar Internacional ISO/IEC 27002:2013 en el Hospital Regional José David Padilla Villafañe E.S.E. de la ciudad de Aguachica-Cesar.

1.1 PLANTEAMIENTO DEL PROBLEMA

Actualmente el hospital se encuentra sistematizando el registro de sus procesos administrativos, financieros y asistenciales, lo que ha llevado a aumentar la plataforma tecnológica en cuanto a equipos de cómputo y comunicaciones, centralizando el almacenamiento de la información y debiendo garantizar la integridad, disponibilidad y confidencialidad de la misma.

Debido a que en el hospital no se cuenta con los suficientes controles ni mecanismos documentados que sirvan de apoyo para contribuir en la mitigación de los problemas de seguridad física y los que hay no han sido debidamente divulgados con el personal que accede a los recursos informáticos, se vienen presentando inconvenientes como desorden en la ubicación de equipos de cómputo, inadecuado control y seguimiento del mantenimiento preventivo de equipos tecnológicos, accesos no autorizados a recursos informáticos y áreas restringidas, falla en los controles anti desastres.

Los anteriores problemas son persistentes puesto que no hay una política clara y que haya sido divulgada para comprometer a los usuarios en la seguridad de la información y demás activos de la empresa y podría conllevar a que exista perdida de activos, daños en los equipos, fallas en la disponibilidad de la información ocasionando fallas en la continuidad del negocio o comprometiendo la confidencialidad de la información.

1.2 FORMULACIÓN DEL PROBLEMA

¿Con la documentación de políticas de seguridad física y ambiental se crearán herramientas que con su utilización eviten el acceso físico no autorizado, daño e interferencia con la información y las áreas del Hospital Regional José David Padilla Villafañe E.S.E. de la ciudad de Aguachica-Cesar?

1.3 OBJETIVOS

1.3.1 Objetivo General

Elaborar políticas de seguridad física y Ambiental basados en el estándar internacional ISO/IEC 27002:2013 en el Hospital Regional José David Padilla Villafañe E.S.E. de la Ciudad De Aguachica-Cesar.

1.3.2 Objetivos Específicos

Diagnosticar los riesgos en cuanto a seguridad física y ambiental que actualmente presenta el Hospital Regional José David Padilla Villafañe E.S.E. de la Ciudad de Aguachica-Cesar.

Definir políticas, controles y mecanismos de seguridad que contribuyan a gestionar los riesgos que se pueden presentar en el Hospital Regional José David Padilla Villafañe E.S.E. de la Ciudad De Aguachica-Cesar.

Desarrollar prueba piloto al objetivo de control 11.2.4 MANTENIMIENTO DE LOS EQUIPOS, para verificación de resultados de la aplicabilidad de las políticas de seguridad.

1.5 JUSTIFICACIÓN

Actualmente las empresas del sector salud tienen características que las diferencian de otros sectores como puede ser la atención al público y que son necesarias tener en cuenta a la hora de desarrollar estrategias que ayudan a dirigir y controlar la empresa para el logro de sus objetivos.

Se pretende dar solución a los problemas de acceso físico no autorizados a la plataforma computacional y de comunicaciones, a los daños e interferencias que puedan presentarse, así como la seguridad de las áreas donde se encuentran ubicados los equipos tecnológicos mediante la elaboración de políticas de seguridad física y ambiental para que posteriormente sean implementadas por el Hospital Regional José David Padilla Villafañe E.S.E del municipio de Aguachica – Cesar, evitando con esto perdidas de activos e información que podrían reflejarse en la interrupción de la continuidad del negocio, garantizando así la estabilidad y seguridad del sistema.

Se presentara la documentación de las Políticas de Seguridad física y ambiental, donde se detalle las buenas prácticas que el HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE ESE debe seguir y cumplir paso a paso para poder mitigar la problemática presentada y así cumplir con los tres principios de la información (integridad, confidencialidad y disponibilidad), permitiendo así el mejoramiento continuo de la empresa.

1.6 HIPÓTESIS

La documentación de políticas de seguridad física y ambiental servirá de herramienta para que con su implementación eviten el acceso físico no autorizado, daño e interferencia con la información y los locales del Hospital Regional José David Padilla Villafañe E.S.E. de la ciudad de Aguachica-Cesar.

1.7 DELIMITACIÓN

1.7.1 Temporal

El proyecto de investigación tiene un tiempo estimado de desarrollo de cinco (5) meses que está comprendido entre agosto de 2014 a diciembre de 2014.

1.7.2 Espacial

Dicho proyecto se desarrolló en la ciudad de Aguachica Cesar, en las instalaciones del Hospital Regional José David Padilla Villafañe E.S.E.

1.7.3 Contextual.

Mapa geográfico de Aguachica

Figura 1. Mapa geográfico de Aguachica

1.7.3.1. Historia de Aguachica

Ciudad de Aguachica - César Altitud: 175 m.s.n.m. Distancia desde Valledupar: 301 Km. Aguachica se encuentra ubicado al sur del departamento del Cesar, entre la cordillera oriental y el valle del río Magdalena, a 301 kilómetros de Valledupar, capital de César. Fue oficialmente fundado el 16 de Agosto de 1748 por José Lázaro de Rivera. Limita al norte con el municipio de La Gloria (César) y El Carmen (Norte de Santander), al este con Río de Oro (César), y al oeste con Gamarra y Morales Bolívar. Es la segunda ciudad después de Valledupar; su estratégica localización la ha convertido en punto de convergencia para la comercialización de los municipios cercanos.

Aguachica constituye el eje económico y administrativo más importante del sur del Departamento del Cesar y parte de los santanderes y el Magdalena; su economía gira alrededor del sector agropecuario, la agroindustria y el comercio en general, lo cual ha permitido el surgimiento de una serie de servicios de apoyo como los agro-técnicos, los financieros, el transporte y otros como los empresariales y personales, dirigidos a los

diferentes sectores económicos y a la población en general; cuenta con un moderno frigorífico, el cual se halla ubicado en el complejo agroindustrial Hitayara en el kilómetro 7 de la vía que de Aguachica conduce a Bucaramanga.

Cómo llegar: Aguachica cuenta con el aeropuerto Hacaritama que recibe vuelos chárter desde diferentes partes del país, sin embargo no es muy usado. Por vía terrestre se puede acceder al municipio desde la Costa Caribe colombiana a través de la vía Santa Marta-Aguachica que comunica a los departamentos de Magdalena y César. Desde el sur del país se llega a través de la vía Bogotá-Bucaramanga-Aguachica que comunica los departamentos de Cundinamarca, Boyacá, Santander y César.

2. MARCO REFERENCIAL

2.1 MARCO HISTORICO

A continuación se referenciarán algunas investigaciones, pertinentes para este estudio:

A nivel internacional: empresas como **Atos Consulting** ofrecen paquetes de consultoría y servicios tecnológicos en el sector salud:
Gestión del Conocimiento y Gestión del Cambio a Plan de formación técnica y experiencia sanitaria, plan de comunicación, plan del cambio y gestión de riesgos.[1]

Tesis de pregrado: "Estandar ISO/IEC 27002 Para Centro De Cómputo De La Facultad De Ingeniería En Electricidad Y Computación (FIEC- ESPOL) ubicada en Quito-Ecuador", julio de 2011 autor: Célida Fabiola Romero Vera ,José Ricardo Castillo Ley , ESCUELA SUPERIOR POLITECNICA DEL LITORAL CENTRO DE EDUCACION CONTINUA.

Resumen: Tesis de pregrado: El trabajo busco orientar e informar al lector en todo lo que corresponde a las buenas prácticas de seguridad de la información.

Tesis de pregrado: "Procedimientos para la auditoría física y medio ambiental de un Data Center basado en la clasificación y estándar internacional TIER"
Autor: Jocelyne Estelita Nogueira Solís, PONTIFICIA UNIVERSIDAD CATOLICA DEL PERU.

Resumen: En este proyecto se presentó la situación actual de los servicios de Data Center brindados en el Perú, demostrando la ausencia de una metodología que pueda ser usada para auditar los mismos y así poder asegurarle al cliente que el Data Center donde está depositando su información la tendrá adecuadamente almacenada y evitando que, de presentarse un riesgo, ésta pueda ser deteriorada o eliminada.

Tesis de pregrado: "Desarrollo de Políticas de Seguridad Informática e Implementación de Cuatro Dominios en Base a la Norma 27002 para el Área de Hardware en la Empresa Uniplex Systems S.A. en Guayaquil"Autor: Erick Abraham Lamilla Rubio, José Roberto Patiño Sánchez, ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL GUAYAQUIL-ECUADOR

Resumen: El presente proyecto tiene como objetivo diseñar e implementar políticas de seguridad informática en base a la normativa 27002 para la empresa Uniplex SA que proporcionan directrices básicas de seguridad de la información, gestión de riesgos y alternativas para su tratamiento.

[1] http://www.es.atosconsulting.com/es-raes/servicios/sectores/salud/gobierno_de_ti_en_organizaciones_de_salud/default.htm

Política seguridad física Sisteseg Bogotá Colombia[2].

Resumen: Prevenir el acceso físico no autorizado, además de evitar daños o robo a los activos de la organización e interrupciones a las actividades del negocio de SISTESEG.

Estudio sobre la seguridad física y lógica del "DATA CENTER" DE LA UNED, UNIVERSIDAD ESTATAL A DISTANCIA[3]

Resumen: el presente estudio se originó en atención al plan de trabajo de la auditoria interna para evaluación de seguridad física y lógica del data center "UNED".

2.2 MARCO CONTEXTUAL

El presente proyecto se realizara en el Hospital José Padilla Villafañe localizado en la Calle 5 No. 30A -56, en la ciudad de Aguachica Cesar, prestando servicios de salud de alta complejidad, dentro del contexto del sistema general de seguridad social en salud.

2.3 MARCO CONCEPTUAL

En el desarrollo de la investigación se manejan, entre otros, los siguientes términos que le conceden al trabajo un sustento conceptual, facilitando la compresión del mismo, a saber:

RIESGO: El riesgo es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre.

Sin embargo los riesgos pueden reducirse o manejarse. Si somos cuidadosos en nuestra relación con el ambiente, y si estamos conscientes de nuestras debilidades y vulnerabilidades frente a las amenazas existentes, podemos tomar medidas para asegurarnos de que las amenazas no se conviertan en desastres[4].

RIESGO = AMENAZA + VULNERABILIDAD - CONTROL

AMENAZA: definida como la probabilidad de ocurrencia de un evento potencialmente desastroso durante cierto período de tiempo en un sitio dado.

VULNERABILIDAD: como el grado de pérdida de un elemento o grupo de elementos bajo riesgo resultado de la probable ocurrencia de un evento desastroso, expresada en una escala desde 0 o sin daño a 1 o pérdida total.[5]

[2] http://www.sisteseg.com/files/Microsoft_Word_-_Politica_Seguridad_Fisica.pdf
[3] http://www.uned.ac.cr/images/auditoria/InformesAI/2012/X-24-2011-02_Seguridad_Fisica_y_Logica_del_Data_Center_de_la_UNED.pdf
[4] http://www.rimd.org/advf/documentos/4921a2bfbe57f2.37678682.pdf
[5] http://www.desenredando.org/public/libros/1993/ldnsn/html/cap3.htm

CONTROL: El termino control hace referencia a un mecanismo preventivo y correctivo adoptado por la administración de una dependencia o entidad que permite la oportuna detección y corrección de desviaciones, ineficiencias o incongruencias en el curso de la formulación, instrumentación, ejecución y evaluación de las acciones, con el propósito de procurar el cumplimiento de la normatividad que las rige, y las estrategias, políticas, objetivos, metas y asignación de recursos. En esencia es preservar la existencia de cualquier organización y apoyar su desarrollo; su objetivo es contribuir con los resultados esperados[6].

POLITICAS DE SEGURIDAD: El objetivo de la Política de Seguridad de Información de una organización es, por un lado, mostrar el posicionamiento de la organización con relación a la seguridad, y por otro lado servir de base para desarrollar los procedimientos concretos de seguridad.[7]

SISTEMA DE INFORMACIÓN: es un conjunto de elementos relacionados entre sí, que se encarga de procesar manual y/o automáticamente datos, en función de determinados objetivos.[8]

TI: Se conoce como tecnología de información a la utilización de tecnología específicamente computadoras para el manejo y procesamiento de información específicamente la captura, transformación, almacenamiento, protección, y recuperación de datos e información.

PLAN: Un plan es una intención o un proyecto. Se trata de un modelo sistemático que se elabora antes de realizar una acción, con el objetivo de dirigirla y encauzarla. En este sentido, un plan también es un escrito que precisa los detalles necesarios para realizar una obra.[9]

ESTRATEGIA: a palabra estrategia deriva del latín strategĭa, que a su vez procede de dos términos griegos: stratos ("ejército") y agein ("conductor", "guía"). Por lo tanto, el significado primario de estrategia es el arte de dirigir las operaciones militares.

Una estrategia muestra cómo una institución pretende llegar a esos objetivos. Se pueden distinguir tres tipos de estrategias, de corto, mediano y largo plazos según el horizonte temporal. Término utilizado para identificar las operaciones fundamentales tácticas del aparato económico.[10]

MODELADO DEL NEGOCIO: Involucra la descripción de la estructura organizacional, procesos de negocios, sistemas de planeación y control, mecanismos de gobierno y administración, políticas y procedimientos de la empresa. Cada uno de estos componentes

[6] http://www.definicion.org/control
[7] http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=4
[8] http://www.incap.org.gt/sisvan/index.php/es/acerca-de-san/conceptos/sistema-de-vigilancia
[9] http://definicion.de/plan/
[10] http://www.aulafacil.com/estrategia/Lecc-2.htm

interactúa y contribuye a alcanzar las metas y objetivos del negocio y provee la base para identificar los requerimientos de los Sistemas de Información (SI) que soportan las actividades del negocio.[11]

PLANEACION ESTRATEGICA: Proceso gerencial que consiste en desarrollar y mantener un ajuste estratégico entre los objetivos y recursos de la empresa y sus oportunidades cambiantes de mercado.

ISO/IEC 27002 Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización

SEGURIDAD FÍSICA: consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial.[12]

2.4 MARCO TEÓRICO

Esta Investigación abarca diferentes teorías, que son de vital importancia para el entendimiento y la realización del mismo, entre éstas se puede mencionar:

2.4.1 PLAN ESTRATÉGICO

El Plan Estratégico es un documento en el que los máximos responsables de una empresa o institución establecen la estrategia a seguir en un periodo plurianual a través de unas líneas de actuación que sirvan de base para la gestión eficaz y eficiente de la organización. En el Plan Estratégico cada línea de actuación debe estar asignada a un responsable de alcanzar los objetivos establecidos con una serie de acciones específicas, así como el tiempo adecuado para llevarla a cabo.[13]

2.4.1.1 Etapas de un Plan Estratégico

Hay dos aspectos claves a considerar para desarrollar un proceso de planificación estratégica:

Enfocar la planificación hacia los factores críticos que determinan el éxito o fracaso de una organización

[11] http://docencia.udea.edu.co/ingenieria/ArquitecturaSoftware/documentos/Del%20Modelo%20Del%20Negocio%20Al%20Modelo%20De%20Requisitos.pdf
[12] http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/2869/1/C7.1373.pdf
[13] http://www.umh.es/plan-estrategico/data/es/definicion.html

Los factores críticos varían de una organización a otra y pueden ser tan diversos como el abastecimiento de materias primas o la cantidad de funcionarios en las horas de mayor demanda.

Diseñar un proceso de planificación que sea realista

Evaluar la experiencia y capacidad técnica que se tiene en planificación y eventualmente pedir asesoría; evaluar el tiempo disponible para realizar el proceso; como también la disposición y compromiso de directivos y funcionarios; y los posibles problemas políticos y organizacionales que pueden aparecer; etc.[14]

2.4.2 Gobernabilidad de ti. Durante muchos años la gobernabilidad ha sido vista como el futuro de las tecnologías de la información y la comunicación, a pesar del manejo de diferentes criterios de calidad en gobernabilidad de TI. El proceso de gobernabilidad de una empresa se refiere al conjunto de responsabilidades y prácticas ejecutadas por el comité directivo de la misma, con el objetivo de proveer dirección estratégica a la compañía, asegurando que los objetivos definidos sean alcanzados, verificando que los riesgos sean administrados apropiadamente y que los recursos utilizados sean utilizados responsablemente. La gobernabilidad de TI es parte integral de la gobernabilidad de la empresa, y comprende el liderazgo, las estructuras organizacionales y los procesos que aseguran que la organización de TI sostenga y extienda las estrategias y objetivos de la organización, siendo responsabilidad del comité directivo de la empresa y del comité ejecutivo de TI.[15]

El gobierno de TI, hace parte del gobierno empresarial. Se define como la estructura de relaciones y procesos para dirigir y controlar la empresa hacia el logro de sus objetivos, por medio de agregar valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre las TI y sus procesos.

El gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que TI en la empresa soporta los objetivos del negocio. Facilita que la empresa aproveche al máximo su información, maximiza los beneficios, capitaliza las oportunidades y gana ventajas competitivas (Palao, 2010).

Son la Junta Directiva y la Gerencia Ejecutiva las responsables del gobierno de TI.
Según el IT Governance Institute, el gobierno de TI tiene cuatro principios fundamentales (ITGI, 2007):

- Dirigir y controlar
- Responsabilidad
- Rendición de cuentas
- Actividades

[14] http://www.infomipyme.com/Docs/GT/Offline/administracion/Planificacion_Estrategica.html
[15] http://www.uptc.edu.co/eventos/2011/eiisi/documentos/memorias_EIISI.pdf#page=75

El gobierno de TI tiene interesados internos y externos, con distintas preocupaciones, a las que el gobierno de TI tiene que darles respuesta. Entre los interesados internos se pueden mencionar al gerente de TI, la junta directiva y los gerentes ejecutivos y de negocios, el gerente de riesgo y cumplimiento y el auditor de TI. Los interesados externos son fundamentalmente los auditores externos, los clientes, los reguladores y los proveedores, cada uno con preguntas e inquietudes particulares.

Las actividades del gobierno de TI se pueden agrupar en cinco áreas de enfoque que son:

- Alineamiento estratégico
- Entrega de valor
- Administración de riesgos
- Administración de recursos
- Medición del desempeño

2.4.2.1 Áreas de enfoque de gobierno de TI

Alineamiento Estratégico: Se enfoca en asegurar el enlace de los planes del negocio y de TI; en definir, mantener y validar la proposición de valor de TI y en alinear las operaciones de TI con las operaciones de la empresa. Según el informe IT Governance Broad Briefing del ITGI, la pregunta clave es si la inversión de una empresa de TI está en armonía con sus objetivos estratégicos (la intención, la estrategia actual y objetivos de la empresa) y por lo tanto la construcción de las capacidades necesarias para ofrecer un valor empresarial. Este estado de la armonía que se conoce como "la alineación." Es complejo, multifacético y nunca del todo logrado.

Entrega de valor: Se refiere a ejecutar la proposición de valor a través de todo el ciclo de entrega, asegurando que TI entrega los beneficios acordados alineados con la estrategia, concentrándose en la optimización de costos, y demostrando el valor intrínseco de TI. Según el informe IT Governance Broad Briefing del ITGI, dice que la entrega de valor de las TI se traduce en entregar a tiempo y dentro del presupuesto. "El valor de IT está en el ojo del espectador".

Administración de Riesgos:

Requiere:

- Conciencia de riesgo por parte de los directores superiores de la empresa.
- Un claro entendimiento del apetito de riesgo de la empresa.
- Un entendimiento de los requerimientos de cumplimiento.
- Transparencia sobre los riesgos significativos de la empresa.
- Implementar las responsabilidades de la administración de riesgos dentro de la organización.

Administración de Recursos: Hace referencia a la inversión óptima y a la adecuada administración de los recursos críticos de TI tales como: aplicaciones, información, infraestructura, datos.

Medición del desempeño: Da seguimiento y supervisa la estrategia de implementación, la finalización de proyectos, el desempeño de procesos y la entrega de servicio. Si no hay forma de medir y evaluar las actividades de TI, no es posible gobernarlas ni asegurar el alineamiento, la entrega de valor, la administración de riesgos y el uso efectivo de los recursos.

2.4.2.2 Marcos de gobierno de TI

A lo largo de la literatura se encuentra un número importante de marcos diseñados para dar soporte a la implementación de distintos aspectos del gobierno de TI; cada uno de ellos enfoca las prioridades en distintos aspectos del gobierno de TI, haciéndolos, en buena medida, complementarios. Sin embargo se pueden revisar tres marcos principales:

- La versión de Cobit©4.1 del IT Governance Institute (ITGI, 2007) que llamaremos simplemente Cobit en adelante, acompañada de ValIT™ del IT Governance Institute (Val IT, 2008) y Risk IT™ del IT Governance Institute (RiskIT, 2009).

- La norma ISO que trata sobre el gobierno corporativo: ISO 38500 (ISO/IEC, 2008)

- El modelo de Calder-Moir (Calder, 2008)

2.4.2.3 Estándares que Apoyan la Gobernabilidad de TI. Los marcos de referencia con herramientas sólidas son esenciales para asegurar que los recursos de TI estén alineados con los objetivos del negocio y que los servicios y la información satisfagan los requisitos de calidad, financieros y de seguridad.

De acuerdo con los marcos de control se observa la presencia de estándares que apoyan el gobierno de TI en alguno de ellos, los que permiten materializar el "cómo" para diferentes controles de TI. Se mencionan a ISO 27001, ISO 27002, ISO 20000, BS 25999, ITIL, PCI DSS, PMBok (Project Management Institute, 2010) CMMI (Phillips, Gallagher, Richter, & Shrum, 2011; Chrissis, Konrad, & Shrum, 2011; Forrester, Buteau, & Shrum, 2011), entre otros. A continuación se presentan algunos de estos estándares: ITIL, ISO 20000 e ISO 27002.[16]

2.4.3 Seguridad Física. Es muy importante ser consciente que por más que la empresa sea la más segura desde el punto de vista de ataques externos (hackers, virus, ataques de DoS, etc.); la seguridad de la misma será nula si no se ha previsto como combatir un incendio o cualquier otro tipo de desastre natural y no tener presente políticas claras de recuperación.

[16] http://albinogoncalves.files.wordpress.com/2011/03/gobierno-de-ti-e28093-estado-del-arte.pdf

La seguridad física es uno de los aspectos más olvidados a la hora del diseño de un sistema informático. Si bien algunos de los aspectos de seguridad física básicos se prevén, otros, como la detección de un atacante interno a la empresa que intenta acceder físicamente a una sala de cómputo de la misma, no. Esto puede derivaren que para un atacante sea más fácil lograr tomar y copiar una cinta de backup de la sala de cómputo, que intentar acceder vía lógica a la misma.

Teniendo las siguientes ventajas:

- ✓ Disminuir siniestros.
- ✓ Trabajar mejor manteniendo la sensación de seguridad.
- ✓ Descartar falsas hipótesis si se produjeran incidentes.
- ✓ Tener los medios para luchar contra accidentes.

Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

2.4.4 Amenazas previstas en Seguridad Física

- ✓ Desastres naturales, incendios accidentales, tormentas e inundaciones
- ✓ Amenazas ocasionadas por el hombre.
- ✓ Disturbios, sabotajes internos y externos deliberados.

2.4.5 Desastre. Interrupción grave en el funcionamiento de una comunidad causando grandes pérdidas a nivel humano, material o ambiental, suficientes para que la comunidad afectada no pueda salir adelante por sus propios medios, necesitando apoyo externo. Los desastres se clasifican de acuerdo a su origen (natural o tecnológico).

2.4.6 Vulnerabilidad. Grado de resistencia y/o exposición de un elemento o conjunto de elementos frente a la ocurrencia de un peligro. Puede ser física, social, cultural, económica, institucional y otros.

2.4.6.1 Vulnerabilidad Física. Está relacionada con la calidad o tipo de material utilizado y el tipo de construcción de las viviendas, establecimientos económicos (comerciales e industriales) y de servicios (salud, educación, sede de instituciones públicas), e infraestructura socioeconómica (central hidroeléctrica, carretera, puente y canales de riego), para asimilar los efectos del peligro.

La vulnerabilidad, es el grado de debilidad o exposición de un elemento o conjunto de elementos frente a la ocurrencia de un peligro natural o antrópico de una magnitud dada. Es la facilidad como un elemento (infraestructura, vivienda, actividades productivas, grado de organización, sistemas de alerta y desarrollo político institucional, entre otros), pueda sufrir

daños humanos y materiales. Se expresa en términos de probabilidad, en porcentaje de 0 a 100.

La vulnerabilidad, es entonces una condición previa que se manifiesta durante el desastre, cuando no se ha invertido lo suficiente en obras o acciones de prevención y mitigación y se ha aceptado un nivel de riesgo demasiado alto.

Para su análisis, la vulnerabilidad debe promover la identificación y caracterización de los elementos que se encuentran expuestos, en una determinada área geográfica, a los efectos desfavorables de un peligro adverso

2.4.7 Mitigar. Reducción de los efectos de un desastre, principalmente disminuyendo la vulnerabilidad.

Las medidas de prevención que se toman a nivel de ingeniería, dictado de normas legales, la planificación y otros, están orientadas a la protección de vidas humanas, de bienes materiales y de producción contra desastres de origen natural, biológicos y tecnológicos

2.4.8 Seguridad Física y del Entorno o Ambiente

2.4.8.1. Áreas Seguras

Evitar el acceso físico no autorizado, daño e interferencia con la información y los locales de la organización.

2.4.8.1.1. Perímetro de Seguridad Física

Control 1: Se deben utilizar perímetros de seguridad (barreras tales como paredes, rejas de entrada controladas por tarjetas o recepcionistas) para proteger las áreas que contienen información y medios de procesamiento de información.

2.4.8.1.2. Controles de Ingreso Físico

Control 2: Las áreas seguras son protegidas mediante controles de ingreso apropiados para asegurar que sólo se le permita el acceso al personal autorizado.

2.4.8.1.3. Asegurar las Oficinas, Habitaciones y Medios

Control 3: Se diseña y aplica la seguridad física para las oficinas, habitaciones y medios.

2.4.8.1.4. Protección contra Amenazas Externas e Internas

Control 4: Se asigna y aplica protección física contra daño por fuego, inundación, terremoto, explosión, revuelta civil y otras formas de desastres naturales o causados por el hombre.

2.4.8.1.5. Trabajo en Áreas Aseguradas. Control 5: Se diseña y aplica la protección física y los lineamientos para trabajar en áreas aseguradas.

2.4.8.1.6. Áreas de Acceso Público, Entrega y Carga

Control 6: Se controlar los puntos de acceso como las áreas de entrega y carga y otros puntos por donde personas no-autorizadas puedan ingresar al local y, se aísla de los medios de procesamiento de información para evitar el acceso no autorizado.

2.4.8.2. Equipo de Seguridad

Se evita pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización.

2.4.8.2.1. Ubicación y Protección del equipo

Control 7: Se ubica o protege el equipo para reducir las amenazas y peligros ambientales y oportunidades para acceso no autorizado.

2.4.8.2.2. Servicios Públicos de Soporte

Control 8: Se protege el equipo de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte.

Las opciones para lograr la continuidad de los suministros de energía incluyen múltiples alimentaciones para evitar que una falla en el suministro de energía.

2.4.8.2.3. Seguridad del Cableado

Control 9: El cableado de la energía y las telecomunicaciones que llevan la data o dan soporte a los servicios de información debieran protegerse contra la intercepción o daño.

2.4.8.2.4. Mantenimiento de Equipo

Control 10: Se debiera mantener correctamente el equipo para asegurar su continua disponibilidad e integridad

2.4.8.2.5. Seguridad del Equipo fuera del Local

Control 11: Se debiera aplicar seguridad al equipo fuera del local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.

El equipo de almacenamiento y procesamiento de la información incluye todas las formas de computadoras personales, organizadores, teléfonos móviles, tarjetas inteligentes u otras formas que se utilicen para trabajar desde casa o se transporte fuera de local normal de trabajo.

2.4.8.2.6. Seguridad de la Eliminación o Re uso del Equipo

Control 12: Se debieran chequear los ítems del equipo que contiene medios de almacenaje para asegurar que se haya retirado o sobre-escrito cualquier data confidencial o licencia de software antes de su eliminación.

Los dispositivos que contienen data confidencial pueden requerir una evaluación del riesgo para determinar si los ítems debieran ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

2.4.8.2.7. Retiro de Propiedad

Control 13: El equipo, información o software no debiera retirarse sin autorización previa.

También se pueden realizar chequeos inesperados para detectar el retiro de propiedad, dispositivos de grabación no-autorizados, armas, etc., y evitar su ingreso al local. Estos chequeos inesperados debieran ser llevados a cabo en concordancia con la legislación y regulaciones relevantes. Las personas debieran saber que se llevan a cabo chequeos inesperados, y los chequeos se debieran realizar con la debida autorización de los requerimientos legales y reguladores.

2.5 MARCO LEGAL

El presente proyecto se basa en las normas y condiciones de la Constitución Política de Colombia en el uso de las aplicaciones y herramientas informáticas las cuales deben ser dirigidas como lo estipula las leyes colombianas y cuáles sus deberes y sanciones.

El proyecto se encuentra enmarcado en la ley 1273 de enero 5 del 2009 en el capítulo I que trata sobre los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

La misma ley en su **artículo 269A**. Hace referencia al acceso abusivo a un sistema informático. Toda persona que logre entrar a un sistema informático que esté protegido o que tenga una medida de seguridad, sin ningún permiso de aquel que tenga el legítimo derecho, para robar o alterar la información incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

En este orden de ideas la citada normal en su **artículo 269c** se refiere a la interceptación de datos informáticos manifestando que el que, intercepte datos informáticos sin ninguna

orden judicial con un sistema informático que los transporte, incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

En relación con los daños informáticos, el **artículo 269D** estipula el que, sin ningún derecho este facultado para destruir, dañe, borre, deteriore, altere o suprima datos informático de un sistema de información incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Sobre el uso del software malicioso el **artículo 269E** de la susodicha ley expresa el que, sin estar facultado para producir, traficar, adquiera, distribuya, venda o envié, software malicioso o dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes; así mismo el **Articulo 269** trata sobre la violación de datos personales manifiesta que la persona que no esté facultado en complicidad de un tercero obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

La norma **ISO/IEC 27002** Este Estándar Internacional establece los lineamientos y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización. Los objetivos delineados en este Estándar Internacional proporcionan un lineamiento general sobre los objetivos de gestión de seguridad de la información generalmente aceptados.

Los objetivos de control y los controles de este Estándar Internacional son diseñados para ser implementados para satisfacer los requerimientos identificados por una evaluación del riesgo.

Este Estándar Internacional puede servir como un lineamiento práctico para desarrollar estándares de seguridad organizacional y prácticas de gestión de seguridad efectivas y para ayudar a elaborar la confianza en las actividades inter-organizacionales.

3. DISEÑO METODOLÓGICO

3.1 TIPO DE INVESTIGACIÓN

Siguiendo la metodología de Hernández, Fernández y Baptista (2003), hay estudios exploratorios, descriptivos, correlaciónales y explicativos.

Este es un estudio descriptivo de enfoque cuantitativo pues se recolectaron datos o componentes sobre diferentes aspectos del personal del Hospital y se realizó un análisis y medición de los mismos.

"La investigación descriptiva busca especificar propiedades, características y rasgos importantes de cualquier fenómeno que se analice"[17].

Así mismo, el estudio tuvo un enfoque cuantitativo, ya que fue necesario para poder analizar los resultados de las encuestas que se aplicaron al personal del Hospital.

3.2 POBLACIÓN

La población para la realización de la investigación estuvo conformada por los empleados de las áreas administrativa, financiera y asistencial que utilizan el computador y el sistema de información de la Institución como herramienta de trabajo, sumando un total de 213 personas.

3.3 MUESTRA

Para efectos de esta investigación se tomó como muestra a 137 empleados, el cual fue el resultado de aplicar la formula estadística:

Figura 2. Formula muestra.

Población Finita

$$n = \frac{Z^2 p \bullet q \bullet N}{Ne^2 + Z^2 p \bullet q}$$

Dónde:

n= tamaño de la muestra	=		**137 empleados**
N= universo	=		213
e=error de estimación	=	0.05	
Z=nivel de confianza	=	95%	= 1.96
p=probabilidad a favor	=		0.5
q=probabilidad en contra	=		0.5

[17] Hernández, Fernández y Baptista, 2003, p. 119

3.4 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

La recopilación de la información necesaria para la estructuración del proyecto se fundamentó en las técnicas de observación, encuesta y lista de chequeo aplicadas al personal que labora en el Hospital José David Padilla Villafañe.

3.5 ANÁLISIS DE LA INFORMACIÓN

Después de aplicados los instrumentos de recolección de datos, se realizó un análisis detallado de los resultados obtenidos y se graficaron para mayor comprensión, además se realizó un cuadro comparativo de los resultados obtenidos en el hospital luego de aplicada la encuesta, lista de chequeo y observación directa con la norma ISO/IEC 27002 de 2013.

3.6 TABLA DE SEGUIMIENTO METODOLÓGICO

Tabla 1.Tabla de seguimiento metodológico

OBJETIVOS	ACTIVIDADES	RESULTADOS
Diagnosticar los riesgos en cuanto a seguridad física y ambiental que actualmente presenta el Hospital Regional José David Padilla Villafañe E.S.E. de la Ciudad de Aguachica-Cesar.	• Aplicar instrumentos de recolección de datos • Interpretación e resultados de los instrumentos aplicado • Comparar los resultados obtenidos en los instrumentos con la norma ISO 27002: 2013 para verificar estado actual del hospital	Encueta, lista de chequeo y registro de observación Gráficos e interpretación de resultados Cuadro comparativo
Definir políticas, controles y mecanismos de seguridad que contribuyan a gestionar los riesgos que se pueden presentar en el	Definir políticas, controles y mecanismos de seguridad Elaborar propuesta de	documentos de políticas de seguridad física y ambiental

Hospital Regional José David Padilla Villafañe E.S.E. de la Ciudad De Aguachica-Cesar.	mejoramiento	Propuesta de Mejoramiento
✓ Desarrollar prueba piloto al objetivo de control 11.2.4 MANTENIMIENTO DE LOS EQUIPOS, para verificación de resultados de la aplicabilidad de las políticas de seguridad.	Preparación de prueba Aplicar Prueba piloto Obtención y presentación de resultados	Comparación de resultados ante y después de la aplicación de la prueba

Fuente: Autores del proyecto.

4. PRESENTACIÓN DE RESULTADOS

4.1. DESCRIPCIÓN Y CARACTERIZACION DEL HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE.

4.1.1 Misión. Nuestro compromiso es la excelente prestación de servicios de salud en la región, participando en el progreso social, científico, económico y docente asistencial de la misma, generando satisfacción a nuestros clientes internos y externos con tecnología de punta y talento humano altamente calificado.

4.1.2 Visión. En el 2016 seremos líderes en la atención de salud de II y III nivel de complejidad, con moderna infraestructura, excelente clima organizacional, calidad y tecnología apoyados en talento humano comprometido, beneficiando a los usuarios de Aguachica y su área de influencia.

4.1.3 Principios corporativos

4.1.3.1 Efectividad en la prestación del servicio

Ofrecemos los mejores servicios técnico-científicos a la comunidad, satisfaciendo las necesidades de nuestros usuarios.

4.1.3.2 Responsabilidad social

Garantizamos a nuestros usuarios atención en salud, independiente de su condición económica y social.

4.1.3.3 Educación

Nuestra entidad participa activamente en la formación del talento humano, buscando una mejor competencia y desempeño.

4.1.3.4 Oportunidad

Asegurar que nuestros usuarios reciban servicios óptimos y a tiempo.

4.1.3.5 Liderazgo

Nuestra organización trabaja activamente para lograr el posicionamiento como los mejores en prestación de servicios de salud en la región.

4.1.3.6 Economía

Nos orientamos hacia una política de sana austeridad y mesura en el gasto público, hacia un equilibrio conveniente y necesario en la inversión, garantizando así la debida proporcionalidad y conformidad de resultados en los términos costo-beneficios.

4.1.4 Valores corporativos

4.1.4.1 Responsabilidad

Los funcionarios del H.J.D.P.V. deben caracterizarse por cumplir sus funciones y prestar los servicios asignados oportunamente con los recursos propios del cargo que desempeña.

4.1.4.2 Compromiso

Los funcionarios asumen cada una de sus obligaciones tanto en sus aciertos como en sus fallas, buscando el mejoramiento continuo y la calidad en los servicios prestados.

4.1.4.3 Honestidad

Los funcionarios se comportan y expresan con coherencia y sinceridad, respetando la verdad y justicia en cada una de sus actuaciones.

4.1.4.4 Solidaridad

Trabajamos en pro de la igualdad, fraternidad, ayuda mutua y la practicamos sin distinción de credo, sexo, raza, nacionalidad o afiliación política, cuya finalidad es el ser humano necesitado.

4.1.4.5 Confianza

Actuamos adecuadamente, generando seguridad en el deber ser y el hacer que garantizan el cumplimiento de nuestra misión.

4.1.4.6 Transparencia

Los funcionarios del HJDPV se caracterizan por prestar los servicios acordes a su plan de cargos, de manera clara, ética y moral en cada uno de sus procesos liderados, los cuales se reflejaran en la calidad de la atención brindada.

4.1.4.7 Respeto

Los trabajadores del HJDPV se caracterizan por prestar sus servicios basados en la dignificación del ser humano, la preservación de la vida, la tolerancia y convivencia pacífica en toda la región.

4.1.4.8 Prudencia

Nuestros funcionarios estarán dispuestos a reflexionar y considerar los efectos que pueden ocasionar sus palabras y acciones, dando como resultado el actuar correcto en cualquier circunstancia.

4.1.4.9 Pertenencia

Nuestros funcionarios inician sus labores con sentido de pertenencia que permita mantener la cohesión humana. Con amor por su trabajo, que además de ser una bendición, es un privilegio hacer parte de esta entidad, participando en las actividades que permitan generar una relación intergrupal, fortaleciendo el sentimiento de que todos somos uno.

4.1.4.10 Lealtad

Los funcionarios son fieles a las políticas, acuerdos y principios éticos por el cual se rige la entidad, buscando el cumplimiento de sus objetivos, con plena conciencia de servicio a la comunidad.

4.1.4.11 Creatividad

Nuestro entorno de trabajo es emocionalmente positivo. Innovamos permanentemente del tal forma que cada una de las áreas funcionales están motivadas a propiciar cambios en el diseño de nuestros servicios.

4.1.4.12 Objetividad

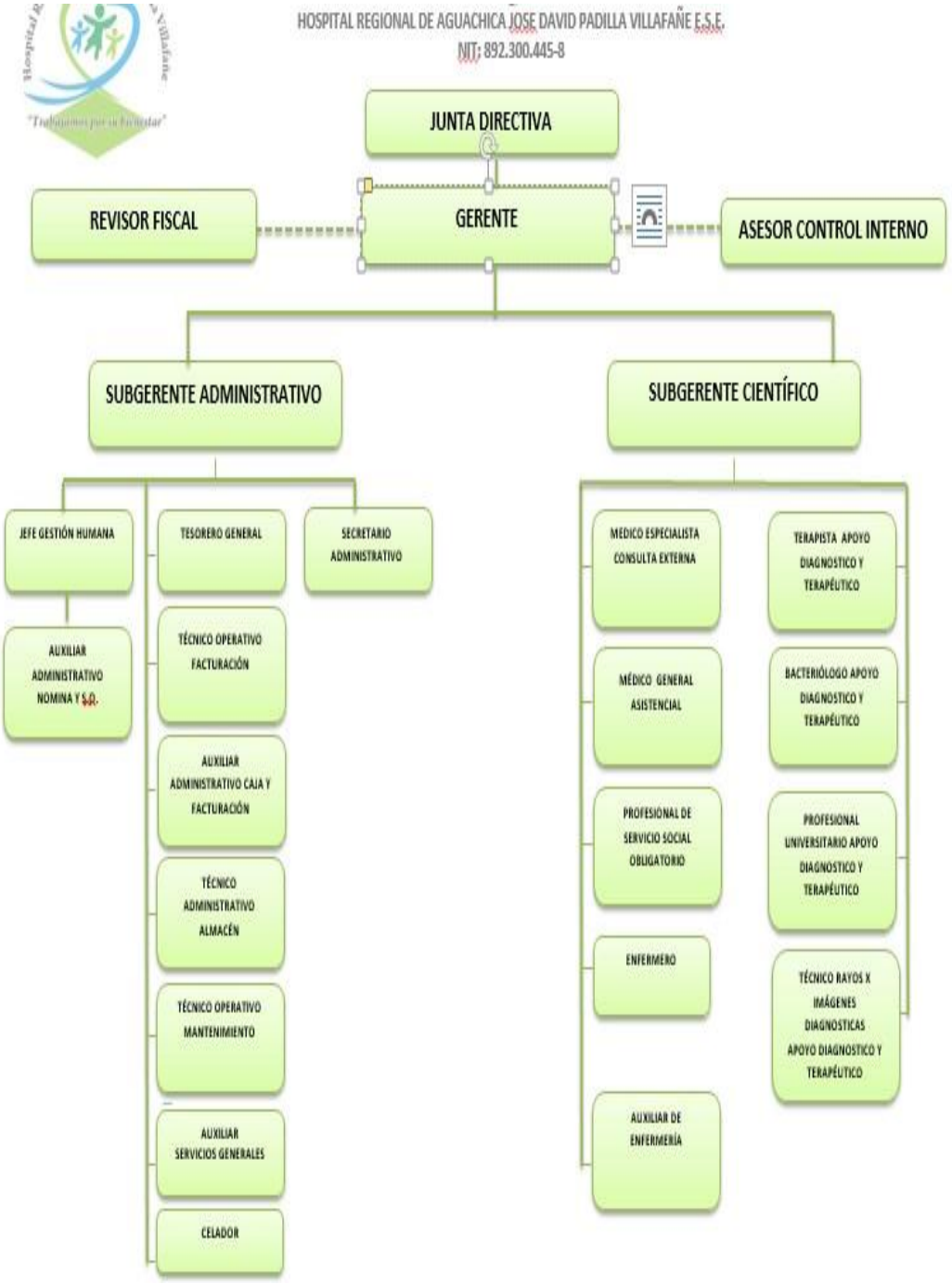
Los funcionarios ven el problema s del entorno con un enfoque que equilibre adecuadamente nuestra realidad, permitiendo ser justos ante los acontecimientos internos y externos, para obrar coherentemente tomando decisiones más eficientes que generen impacto en la región.

4.1.4.13 Servicio

Somos conscientes que nuestra principal responsabilidad es brindar atención en salud con calidad y calidez, satisfaciendo las necesidades y expectativas del paciente, familia y comunidad.

4.1.5 Organigrama de la organización

Figura 3.



4.2 DIAGNÓSTICO DE LA SEGURIDAD DE LA INFORMACIÓN FÍSICA Y DEL AMBIENTE DEL HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE.

Para la realización del diagnóstico se realizó como apoyo una auditoria al hospital sobre el dominio "**SEGURIDAD FÍSICA Y AMBIENTAL"** basados en el estándar internacional ISO/IEC 27002:2013, la cual se encuentra en los anexos del presente proyecto.

Matriz de riesgos. Código identificador del riesgo.

El código de identificación nos permite trabajar de forma estandarizada y ser incluido en una base de datos de riesgos. Este podría tener, por ejemplo, la estructura RX999, donde 999 es un consecutivo y la "X" es la Categoría del Riesgo:

RA: Riesgo de Administración
RE: Riesgo Externo
RO: Riesgo Organizacional
RT: Riesgo Técnico

Causa del riesgo

El evento que causa el riesgo. Nivel más bajo de la RBS (Estructura de Desglose del Riesgo) que se establece. En caso de no existir en la RBS, señalar en fuente de color rojo, con el objetivo de actualizar posteriormente la RBS para futuros proyectos
Descripción del Riesgo.

Las características y la forma en que se especifican los riesgos varían según la organización. Para esta práctica utilice la siguiente sintaxis: Si sucede el evento que consecuencias sobre los objetivos del proyecto traería.

Tabla 2. Probabilidad.

Muy Probable	0.9
Bastante Probable	0.7
Probable	0.5
Poco Probable	0.3
Improbable	0.1

Fuente: Autores del proyecto

Tabla 3. Impacto

Muy Alto	0.8
Alto	0.4
Moderado	0.2
Bajo	0.1
Muy Bajo	0.05

Fuente: Autores del proyecto

Tabla 4. Marcador de riesgo para un riesgo específico

(P x I)

Impacto	Muy bajo	Bajo	Moderado	Alto	Muy Alto
Probabilidad	.05	.1	.2	.4	.8
0.9	0.05	0.09	0.18	0.36	0.72
0.7	0.04	0.07	0.14	0.28	0.56
0.5	0.03	0.05	0.10	0.20	0.40
0.3	0.02	0.03	0.06	0.12	0.24
0.1	0.01	0.01	0.02	0.04	0.08

Verde: Riesgo Bajo – Amarillo: Riesgo Moderado – Rojo: Riesgo Alto

Fuente: Autores del proyecto

Combinando las escalas de la probabilidad y del impacto obtenemos la matriz PxI, que se muestra arriba, la cual nos permite calificar cada riesgo según la escala:

Tabla 5. Riesgo.

Alto	0.99 - 0.18
Moderado	0.17 - 0.05
Bajo	0.04 - 0.01

Fuente: Autores del proyecto

Probabilidad.

Para cada riesgo, utilizando la escala de probabilidad, le asignamos el valor correspondiente.

Impacto.

Para cada riesgo, utilizando la escala de impacto, le asignamos el valor correspondiente.

Rango (PxI).

Multiplicación de la probabilidad por el impacto.

Señales.

En la manera de lo posible indicar una señal de que el riesgo va a suceder.

Responsable.

Miembro del equipo o de la organización que debe responder por la ejecución de las Acciones planeadas para ese riesgo.

Una vez aplicado los instrumentos de recolección de datos como: encuesta a los empleados del HOSPITAL José David Padilla Villafañe De Aguachica-Cesar se hizo notable un análisis de la información Suministrada, la cual se encontraron riesgos, que pueden afectar la seguridad de la Información contenida en el HOSPITAL.

Se evidencia en los resultados que los riesgos a los que se enfrenta el HOSPITAL son de un nivel alto; por consiguiente, se debe mejorar o tomar medidas al respecto, para evitar que la organización sea vulnerable a cualquier tipo de amenaza que afecte su activo más importante que es la información.

A continuación, se muestra el análisis de los riesgos, con su respectivo impacto y probabilidad.

4.3 EVALUACION DE RIESGOS

CÓDIGO	CAUSA	DESCRIPCIÓN DEL RIESGO	PROBABILIDAD	IMPACTO	PxI	ESTRATEGIAS	ACCIONES	RESERVAS	RESPONSABLE	SEÑALES
RO-01	Adquirir y Mantener infraestructura Tecnologica-Infraestructura de TI	si no se tiene socializada las politicas de seguridad que tiene el centro de computo, **se puede** encurrir en errores que afectan el buen funcionamiento del sistemas y la informacion.	0,7	0,4	0,28	ACEPTAR-MITIGAR	Elaboración de un documento que describa los lineamientos que se deben tener en cuenta para la seguridad de la información	Para el Tratamiento de Los riesgos Identificados Durante el Proyecto se Establecerá un Plazo de 30 Días para Cumplir con Las entregas de Las capacitaciones	JEFE DE SISTEMAS	Desconocimiento en Competencias De las politicas.
RO-02	Controles del entorno de TI	Si el Hospital no cuenta con las protecciones necesarias para evitar daños por fuego, y si no se cuenta con sensores automáticos que contribuyan para una rápida reacción advirtiendo la presencia de factores externos que causantes de desastres (alarmas, sensores), y si no ha recibido capacitación para el manejo de los mismos, **esto puede** ocaccionar perdida equipos y de informacion .	0,7	0,8	0,56	ACEPTAR-MITIGAR	Elaboración de un documento que describa los lineamientos que se deben tener en cuenta para la seguridad de la información.	Para el tratamiento de los riesgos identificados durante el proyecto se establecerá un 10 % del valor del proyecto. En caso de que estos no requieran inversión económica el dinero debe ser reembolsado a la organización.	JEFE DE SISTEMAS	No existe un plan de contingencia, para mitigar los diferentes accidentes que se puedan presentar.
RO-03	Limpieza del puesto de trabajo.	Si no se cuenta con una metodología estandar acerca de la prohibicones sobre la ingesta de alimentos y de factores ambientales o externos, así como la falta de impermeabilización techo,**esto puebe** ocacionar daños en los equipos que procesan la informacion ocacionando perdida de hardware o daños parciales y lo mas importante perdida de informacion.	0,7	0,8	0,56	ACEPTAR-MITIGAR	Socialización de la política de ingesta de alimentos en el puesto de trabajo.	Para el Tratamiento de Los riesgos Identificados Durante el Proyecto se Establecerá un Plazo de 30 Días para Cumplir con Las entregas de Las capacitaciones	JEFE DE SISTEMAS	Suciedad, deterioro del equipo de cómputo.

RO-04	Mantener equipos tecnologicos	si no se socializan las politicas que regulen la salida de los equipos de computo **esto puede** ocacionar perdida o robos de dichos equipos y de informacion valiosa para el empleado y empresa.	0,7	0,8	0,56	ACEPTAR-MITIGAR	implementar y diligenciar las respectivas planillas para la salida de los equipos de dentro y fuera de la institucion, para evitar incidentes informáticos.	Para el Tratamiento de Los riesgos Identificados Durante el Proyecto se Establecerá un Plazo de 30 Días para Cumplir con Las entregas de Las capacitaciones	JEFE DE SISTEMAS O RESPONSABLE DE LA OPERACIÓN DEL SISTEMA DE INFORMACION(INGENIERO DE SISTEMAS)	Sensibilidad de la empresa a las amenazas y riesgos informáticos a los que se ven expuesto día a día
RO-05	Mecanismos de seguridad para el control de acceso a la empresa	si las area administrativa y asistencial no se lleva un control a la presencia de terceros sin previa autorización y supervisión, **esto puede** que los equipos queden desatendidos y vulnerables, debido que cualquiera pueda manipular la informacion o extraer algun objeto de las misma.	0,5	0,2	0,1	ACEPTAR-MITIGAR	Implementar un mecanismo de seguridad como: Carnet de visitante y tiempo de permanencia máximo en la organización, con el fin de tener un control más exacto del ingreso del	Para el Tratamiento de Los riesgos Identificados Durante el Proyecto se Establecerá un Plazo de 30 Días para Cumplir con Las entregas de Las capacitaciones	JEFE DE CADA DEPENDENCIA	Usuarios dentro de la empresa, sin ningún tipo de identificación y actividades a realizar.
RO-06	Controles para el ingreso de personal no autorizado	Si no se establece un parametro de identificacion por parte de los empleados, **esto puede** dificultar la identificacion de persona que estan permitidas entrar a las diferentes areas.	0,7	0,2	0,14	ACEPTAR-MITIGAR	Implementar un mecanismo de seguridad como: Carnet de visitante y tiempo de permanencia máximo en la organización, con el fin de tener un control más exacto del ingreso del personal externo	Para el Tratamiento de Los riesgos Identificados Durante el Proyecto se Establecerá un Plazo de 30 Días para Cumplir con Las entregas de Las capacitaciones	JEFES DE CADA DEPENDENCIA - EMPLEADOS	Usuarios dentro de la empresa, sin ningún tipo de identificación y actividades a realizar.

RT-02	Inventario de activos.	si no se tiene socializada el plan de mantenimiento preventivo y su ejecucion como se debe realizar **se puede** encurrir en errores que afectan el buen funcionamiento del hardware y sistemas para la informacion que ahi se maneja	0,5	0,2	0,1	MITIGAR	Actualización periódica de los activos de la organización	Para el Tratamiento de Los riesgos Identificados Durante el Proyecto se Establecerá un Plazo de 30 Días para Cumplir con Las entregas de Las capacitaciones	JEFE DE SISTEMAS	Robo de activos de la empresa, no existe un responsable de los mismos
RT-03	Riesgo Adquirir y Mantener Infraestructura Tecnologica-Proteccion	Las áreas están protegidas por un perimetro de seguridad física adecuado.	0,3	0,1	0,03	MITIGAR	permanecer bajo llave las dependencias cuando no hayan empleados laborando en ellas.	Para el Tratamiento de Los riesgos Identificados Durante el Proyecto se Establecerá un Plazo de 30 Días para Cumplir con Las entregas de Las capacitaciones	JEFES DE CADA DEPENDENCIA - EMPLEADOS	Ahí exepciones con respecto a las estaciones de enfermeria que no pueden estar delimitadas.
RT-04	Recursos de TI	si se cuenta con los controles adecuados para controlar el acceso no autorizado a las áreas esto ayuda a controlar el acceso al público y mitigar manipulacion de equipos e informacion a personal no autorizado.	0,3	0,1	0,03	MITIGAR	Cambio de contraseñas periódicas, que cumplan con los requisitos que debe tener como: Mayúsculas, minúsculas, números y caracteres.	Para el Tratamiento de Los riesgos Identificados Durante el Proyecto se Establecerá un Plazo de 30 Días para Cumplir con Las entregas de Las capacitaciones	JEFES DE CADA DEPENDENCIA - EMPLEADOS	Existen equipos sin contraseña.
			PROMEDIO		**0,27**					
			CALIFICACION GENERAL DEL RIESGO: **ALTO**							

4.4 CUADRO COMPARATIVO DE VERIFICACIÓN DE ESTADO ACTUAL DEL HOSPITAL

Se realizó una comparación entre los resultados obtenidos luego de la aplicación de los instrumentos de recolección de datos y el análisis a los mismos contra la norma ISO 27002:2013 en su dominio "11. SEGURIDAD FISICA Y AMBIENTAL", evidenciando los resultados que a continuación se detallarán.

Tabla 6. Cuadro De Comparación

CONTROL NORMA	RESULTADOS HOSPITAL	CUMPLIMIENTO
11.1.1 Perímetro de seguridad física	Se determinó en un gran porcentaje que las áreas están protegidas por un perímetro de seguridad física adecuado a excepción de las estaciones de enfermería puesto que estos no deben tener puerta que obstruyan la rápida reacción del personal asistencial.	TOTAL
11.1.2 Controles de acceso físico	Se determinó que en el centro de cómputo se cumple a cabalidad los controles de acceso físico, sin embargo los empleados de las demás áreas no portan el carnet que los identifique como empleados de la Institución dejando así una brecha en la seguridad de las áreas.	PARCIALMENTE
11.1.3 Seguridad de oficinas, despachos y recursos.	Se evidencio que en el centro de cómputo existe el documento políticas de seguridad de la información, sin embargo al indagar con los empleados, el 75% manifestó no conocer dichas políticas ni se encontró evidencia de la divulgación de las mismas.	PARCIALMENTE
11.1.4 Protección contra las amenazas externas y ambientales.	Si bien el Hospital cuenta con las protecciones necesarias para evitar daños por fuego, no se cuenta con sensores automáticos que contribuyan para una rápida reacción advirtiendo la presencia de factores externos causantes de desastres (alarmas, sensores), además se evidencia que el 20% de los empleados encuestados desconocen la ubicación de los extintores y el 63% nunca ha	PARCIALMENTE

	recibido capacitación para el manejo de los mismos.	
11.1.5 El trabajo en áreas seguras.	El Hospital cuenta con los controles adecuados para el trabajo en áreas seguras.	TOTAL
11.1.6 Áreas de acceso público, carga y descarga.	El hospital cuenta con los controles adecuados para controlar el acceso no autorizado a las áreas de carga, despacha y acceso al público.	TOTAL
11.2.1 Emplazamiento y protección de equipos.	Se notó grandes falencias puesto que el 15% de los encuestados manifestó no tener conocimiento sobre alguna directriz que le impidiera comer, beber o fumar cerca de los equipos de cómputo, ni se encontró la presencia de dispositivos que protejan contra rayos y/o adviertan niveles inadecuados de factores ambientales o externos, así como la falta de impermeabilización techo.	NO CUMPLE
11.2.2 Instalaciones de suministro.	El Hospital cuenta con los controles adecuados para la protección contra fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro.	TOTAL
11.2.3 Seguridad del cableado.	El Hospital cuenta con los controles adecuados para brindar seguridad al cableado de datos y energía eléctrica.	TOTAL
11.2.4 Mantenimiento de los equipos.	Si bien existe el documento "plan de mantenimiento preventivo", no se evidencio la divulgación del mismo, la ejecución se refleja parcialmente en las planillas de mantenimiento y no se encontró registro de seguimiento a dicho plan, por el contrario el 95% de los empleados encuestados afirmo no conocer las fechas estipuladas para el mantenimiento a los equipos a su cargo. Más aun el 50% de los empleados no se encuentran satisfechos con el mantenimiento de sus equipos. No se encuentra evidencia que demuestre que los mantenimientos fueron realizados en verdad.	PARCIALMENTE
	Se observó que aunque solo el 35%	

11.2.5 Salida de activos fuera de las dependencias de la empresa.	de los empleados encuestados dicen conocer políticas que reglamenten la salida de equipos de cómputo de las dependencias del Hospital, no se encuentra documento alguno que reglamente dicha política.	NO CUMPLE
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Se observó que aunque solo el 35% de los empleados encuestados dicen conocer políticas que reglamenten la salida de equipos de cómputo del Hospital, no se encuentra documento alguno que reglamente dicha política.	NO CUMPLE
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.	El Hospital cuenta con los controles adecuados para verificar la seguridad en la reutilización de los equipos que contengan información sensible de la entidad.	TOTAL
11.2.8 Equipo informático de usuario desatendido.	Aunque en las áreas administrativas y centro de cómputo no se permite la presencia de terceros sin previa autorización y supervisión, el 14% de los encuestados correspondientes al área asistencial manifestó lo contrario debido a que por la ubicación de su área la presencia de pacientes es muy alta y en momentos de emergencia donde el personal de atención se desplace de su área, quedan los equipos desatendidos y vulnerables, siendo el único mecanismo de seguridad el circuito cerrado de televisión.	PARCIALMENTE
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	Se observó que el 19% de los empleados encuestados afirmo no cerrar su sesión de trabajo en el equipo de cómputo utilizado cuando se ausenta de su puesto, creando así una vulnerabilidad hacia la integridad y confidencialidad de la información. En cuanto al puesto de trabajo despejado se hayo que nadie deja sobre su escritorio documentos sensibles para la entidad en el momento que se ausentan de su área de trabajo.	PARCIALMENTE

Fuente: Autores del proyecto

4.5 POLITICAS DE SEGURIDAD FISICA Y DEL AMBIENTE

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN (SEGURIDAD FISICA Y AMBIENTAL)

Generalidades

La información es un recurso que, como el resto de los activos, tiene valor para la Institución y por consiguiente debe ser debidamente protegida.

Las Políticas de Seguridad de la Información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información y de la operación de la Institución, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de la misma.

Es importante que los principios de la Política de Seguridad sean parte de la cultura Institucional.

Para esto, se debe asegurar un compromiso manifiesto de las máximas Autoridades del Hospital y de los jefes de áreas para la difusión, consolidación y cumplimiento de la presente Política.

Objetivo

Proteger los recursos de información del Hospital Regional José David Padilla Villafañe y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad, legalidad y confiabilidad de la información.

Asegurar la implementación de las medidas de seguridad comprendidas en esta Política, identificando los recursos y las partidas presupuestarias correspondientes, sin que ello implique necesariamente la asignación de partidas adicionales.

Mantener la Política de Seguridad del Organismo actualizada, a efectos de asegurar su vigencia y nivel de eficacia.

Alcance

Las políticas definidas en el presente documento aplican para todos los funcionarios públicos y contratistas, a todos sus recursos y a la totalidad de la información que se genere de los procesos de la institución, mediante el uso y/o utilización del recurso informático del Hospital Regional José David Padilla Villafañe.

Responsabilidad

Consciente de sus necesidades actuales, el Hospital Regional José David Padilla Villafañe implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios y de negocio vigentes.

Todos los funcionarios del Hospital Regional José David Padilla Villafañe sea cual fuere su nivel jerárquico o forma de vinculación, son responsables de la implementación de esta Política de Seguridad de la Información dentro de sus áreas de responsabilidad, así como del cumplimiento de dicha Política por parte de su equipo de trabajo.

La Política de Seguridad de la Información es de aplicación obligatoria para todo el personal del Hospital, cualquiera sea su situación de revista, el área a la cual se encuentre afectado y cualquiera sea el nivel de las tareas que desempeñe.

Esta política será revisada con regularidad como parte del proceso de revisión gerencial, o cuando se identifiquen cambios en el negocio, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN (SEGURIDAD FISICA Y AMBIENTAL)

El HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE ha establecido las siguientes Políticas de Seguridad de la Información Física y Ambiental, las cuales representan la visión de la Institución en cuanto a la protección de sus activos de Información:

Cualquier persona que tenga acceso a las instalaciones del Hospital, deberá registrar en el libro de minutas de portería al momento de su entrada, el equipo de cómputo, equipo de comunicaciones 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.

Será responsabilidad de los funcionarios de las áreas, supervisar o inspeccionar a los visitantes que ingresan a su área laboral. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyendo al visitante en el momento de ingreso sobre los requerimientos de seguridad del área.

Para el acceso al centro de cómputo, se deberá supervisar o inspeccionar por parte del encargado a los visitantes durante todo el tiempo que dure dicha visita, de igual manera se deberá registrar la planilla de ingreso. Sólo se permitirá el acceso mediando propósitos específicos y autorizados e instruyéndose al visitante en el momento de ingreso sobre los requerimientos de seguridad del área.

Será responsabilidad de los funcionarios de las áreas en las que se almacene o procese información, controlar y limitar el acceso a la misma, cuando esta sea clasificada o confidencial, exclusivamente a las personas autorizadas.

Todo el personal que labore en el hospital, deberá portar el carnet institucional en un lugar visible.

Para el ingreso a las instalaciones del hospital por parte de visitantes, se entregaran tarjetas en recepción en portería para el acceso de los mismos, señalando el área al cual tendrán autorización.

Sera responsabilidad del personal que labora en las distintas áreas del hospital, garantizar que las puertas y ventanas permanecerán cerradas y aseguradas cuando no haya vigilancia.

Será responsabilidad del jefe del área de sistemas, almacenar los equipos redundantes y la información de resguardo (back up) en un sitio seguro y distante del lugar de procesamiento, según lo indica el manual de procedimientos del área de sistemas, para evitar daños ocasionados ante eventuales contingencias en el sitio principal.

Las áreas vacías en las que se almacene o procese información deberán permanecer cerradas físicamente bajo llave y revisadas periódicamente por el encargado del área.

El acceso a las áreas de entrega y carga desde fuera del Hospital, solo se permitirá al personal identificado y autorizado por el responsable del área relacionada en dicho proceso.

Se deberá inspeccionar por quien recibe, el material que ingresa al hospital, para evitar amenazas potenciales antes que el material sea trasladado del área de entrega y carga al punto de uso.

Se deberá registrar el material que ingresa en concordancia con los procedimientos de gestión de activos a su ingreso al local.

Los usuarios no deben mover o reubicar los equipos de cómputo o de telecomunicaciones, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización del área de sistemas. En caso de requerir este servicio deberá notificarlo a dicha área.

El área de Almacén, será la encargada de generar el resguardo y obtener la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada.

El equipo de cómputo asignado, deberá ser para uso exclusivo de las funciones inherentes en el hospital.

Es responsabilidad de los usuarios almacenar la información únicamente en la carpeta de disco duro identificada como "Mis Documentos", ya que las otras están destinadas para archivos de programa y sistema operativo.

En las áreas en las que se manejen equipos de cómputo y/o electrónicos, no se deberán consumir alimentos, ingerir líquidos ni fumar.

Se debe evitar colocar objetos encima del equipo tecnológico o cubrir los orificios de ventilación del monitor o del CPU.

Sera responsabilidad del usuario responsable del equipo mantenerlo e en un entorno limpio y sin humedad.

El usuario debe asegurarse que los cables de conexión no sean pisados o pinchados al colocar otros objetos encima o contra ellos.

Cuando se requiera realizar cambios múltiples del equipo de cómputo derivado de reubicación de lugares físicos de trabajo, éstos deberán ser notificados con una semana de anticipación al área de sistemas a través de un plan detallado de movimientos debidamente autorizados por el jefe del área que corresponda como lo indica el manual de procedimientos de sistemas.

Queda prohibido que el usuario no autorizado abra o desarme los equipos tecnológicos.

Los usuarios encargados de las áreas seguras deberán monitorear las condiciones ambientales; tales como temperatura y humedad, que pudiera afectar adversamente la operación de los medios de procesamiento de la información.

Únicamente el personal autorizado por el área de sistemas, podrá llevar a cabo los servicios y reparaciones al equipo tecnológico, por lo que los usuarios deberán solicitar la identificación del personal designado antes de permitir el acceso a sus equipos.

Los usuarios responsables de los equipos deberán asegurarse de respaldar 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.

Los usuarios deberán tener los equipos de tecnológicos registrados a su cargo, dispuestos para la realización de los mantenimientos preventivos en las fechas indicadas o concordar nuevas fechas con el área de sistemas si existe algún improviso que impida la realización del mantenimiento en las fechas estipuladas.

Será obligación del área de sistemas velar por la correcta ejecución del plan de mantenimiento preventivo o en casos de incumplimiento informar al área de auditoria interna la causa y dejar registro de la notificación.

Se deberá llevar por el área de sistemas, registro de todos los mantenimientos tanto preventivos como correctivos realizados a equipos tecnológicos, detallando los procedimientos realizados y hallazgos encontrados, en la planilla definida para tal fin.

Para el retiro de equipos tecnológicos fuera de sus áreas asignadas, se deberá tener previa autorización del usuario responsable del activo y del jefe de área.

Los empleados, contratistas y terceras personas que tienen la autoridad para permitir el retiro de los activos fuera de las áreas, deberán estar claramente identificados.

Se deberá establecer límites de tiempo para el retiro del equipo y se debe realizar un chequeo de la devolución.

Cuando un equipo deba ser retirado del área definitivamente, el usuario responsable del mismo deberá notificar por escrito al área de almacén para que este le sea retirado del inventario a su cargo.

Para el retiro de equipos tecnológicos fuera de las instalaciones del hospital, se deberá tener previa autorización escrita del usuario responsable del activo, jefe de área, jefe de almacén y jefe del área de sistemas.

En el caso que un equipo sea dado de baja, será responsabilidad del área de sistemas, garantizar que sus dispositivos de almacenamiento serán sobrescritos en caso de reutilizarlos o de lo contrario físicamente destruidos para evitar la pérdida de confidencialidad de la información registrada en ellos.

Todos los usuarios serán responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto, la cual se podrá desbloquear sólo con la contraseña del usuario. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados.

Será responsabilidad del área de sistemas, configurar los computadores para que se inactive la sesión de usuario en un tiempo determinado.

Sera responsabilidad de los funcionarios, no dejar abandonada en las impresoras información confidencial y secreta, una vez se haya impreso.

Los escritorios o puestos de trabajo deben mantenerse limpios y sin documentos fuera del horario de trabajo o en ausencia prolongada del sitio, esto para evitar el acceso no autorizado a la información.

Es responsabilidad de todos los funcionarios y contratistas del HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE reportar los Incidentes de Seguridad, eventos sospechosos y el mal uso de los recursos que identifique.

Las violaciones a las Políticas y Controles de Seguridad de la Información serán reportadas, registradas y monitoreadas.

A los equipos portátiles personales no se les brindará soporte de ninguna índole: ni de hardware ni de software, porque no son responsabilidad de la entidad por ende el dueño debe hacerse cargo y responsable de su computador.

Los funcionarios que tengan asignado cualquier equipo tipo portátil, deben hacer correcto uso de los mismos y de la información que contienen, porque dadas las características de ese tipo de tecnología, se presentan más vulnerabilidades de seguridad, por las facilidades de conectarse diferentes ambientes informáticos, en los cuales la institución no tiene control, y adicionalmente son más susceptibles a robo o pérdida.

Los equipos de computación portátiles asignados tienen carácter intransferible y son de responsabilidad del personal respectivo, por tanto no se pueden realizar préstamos de estos equipos.

Las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a las oficinas solo deben ser utilizadas por los funcionarios autorizados y, salvo situaciones de Emergencia, estos no deben ser transferidos a otros funcionarios de la Entidad, Contratista o Terceros con su debida autorización.

4.6 PLAN DE MEJORAMIENTO

PLAN DE MEJORAMIENTO

SEGURIDAD FISICA Y AMBIENTAL
ISO/IEC 27002:2013
HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE ESE.

Teniendo en cuenta los hallazgos presentados durante la auditoría realizada, se presenta a continuación el siguiente plan de mejoramiento para la mitigación del riesgo presentado.

Se deberá requerir que todos los usuarios, contratistas, terceras personas y todos los visitantes usen alguna forma de identificación visible. Para los empleados deberá exigirse la portabilidad del carnet que lo acredite como trabajador de la Institución

Exigir a las empresas contratistas del personal que labora en el Hospital, que para poder ejecutar el objeto de su contrato deberán allegar inicialmente a la oficina de Gestión Humana de la Institución, el documento que acredita la carnetización de todos sus empleados.

El documento de política de seguridad de la información deberá ser aprobado por la gerencia, publicado y comunicado a todos los empleados y las partes externas relevantes.
Implementar mecanismos que permitan divulgar inmediatamente las políticas de seguridad al personal que interviene en ellas.

Se deberá implementar una planilla en la que se registre al personal que participo de la divulgación de las políticas de seguridad.

Para la incorporación de nuevo personal al Hospital, se deberá entregar a estos, documento con las políticas de seguridad del hospital y a su vez dejar constancia de la divulgación de las mismas.

Revisar las políticas de seguridad en intervalos planeados o si ocurren cambios significativos para asegurar su continua idoneidad, eficiencia y efectividad; de registrarse cambios, estos deberán ser divulgarlos inmediatamente al personal relevante.

Implementar inmediatamente un sistema que permita monitorear factores externos que influyan o interrumpan con la integridad del centro de cómputo, usando sensores de humedad, de fuego, alarmas entre otros.

Realizar jornadas que contribuyan al reconocimiento de la ubicación de los extintores de fuego con el personal del Hospital.

Capacitar a todo el personal que labora en la Institución sobre el correcto uso de los extintores de fuego, a su vez programar y realizar con el acompañamiento del cuerpo de bomberos simulacros de incendios periódicamente.

Registrar evidencias de capacitación y asistencias a los diferentes simulacros.

Asegurar que todos los empleados y las partes externas relevantes del hospital conozcan las políticas de seguridad que prohíban el comer, beber o fumar cerca de los equipos de cómputo.

Se debe implementar una planilla en la que se registre al personal que participo de la divulgación de las políticas.

Realizar un estudio que determine la necesidad de implementar un sistema de protección contra rayos y de ser viable implementarlo.

Divulgar el plan de mantenimiento con los empleados y áreas responsables de los equipos de cómputo.

Registrar la planilla que certifique la divulgación del plan de mantenimiento.

Posterior a la ejecución de las tareas descritas en el plan de mantenimiento preventivo de equipos de cómputo, se deberá diligenciar totalmente la planilla definida por el área de sistemas y así acreditar las tareas realizadas. La planilla deberá firmarse por la persona encargada del mantenimiento y el responsable de dicho equipo.

Se deberá comparar periódicamente por el jefe del área de sistemas el plan de mantenimiento con las planillas de ejecución para garantizar el cumplimiento de dicho plan y elaborar actas con los resultados de la comparación realizada.

Actualizar las políticas de seguridad periódicamente, incluyendo las necesarias para reglamentar la salida de equipos de cómputo de las dependencias del Hospital, divulgarlas resaltando la responsabilidad que adquiere el personal de la Institución y registrar evidencias de dicha divulgación.

Cubrir permanentemente con guardias de seguridad y circuito cerrado de televisión aquellas áreas en las que por necesidad del servicio son áreas abiertas y susceptibles a la presencia de personal no autorizado.

Programar los computadores para que se inactive la sesión a determinado tiempo de inactividad.

4.7 PRUEBA PILOTO AL OBJETIVO DE CONTROL 11.2.4 MANTENIMIENTO DE LOS EQUIPOS.

Para comprobar la eficacia de las políticas y el plan de mejoramiento presentado, se realizó una prueba piloto al objetivo de control **11.2.4 MANTENIMIENTO DE LOS**

EQUIPOS obteniendo resultados satisfactorios frente al estado anterior en el que se encontraba el Hospital.

Como evidencia de la prueba piloto, se presentan los siguientes documentos:

Plan de mantenimiento equipos de cómputo.

Planillas de ejecución mal diligenciada e incompleta

Resolución plan de mantenimiento

Divulgación plan de mantenimiento

Plantillas de ejecución correctamente diligenciadas

Actas de comparación plan de mantenimiento Vs plantilla de ejecución

Fotografías equipos antes y después de la adopción de políticas y plan de mejoramiento.

Encuesta

Tabla 7. Plan de mantenimiento equipos de cómputo.

PLAN DE MANTENIMIENTO PREVENTIVO DE EQUIPOS DE COMPUTO 2015					
DESCRIPCION	**UBICACIÓN**	**PERIOCIDAD**	**FECHA**	**RESPONSABLE**	**ACTIVIDAD**
PC DE ESCRITORIO	ARCHIVO 1	BIMENSUAL	03/01/2015 04/04/2015 04/07/2015 03/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	ARCHIVO 2	BIMENSUAL	03/01/2015 04/04/2015 04/07/2015 03/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONSULTORIO 1	BIMENSUAL	03/01/2015 04/04/2015 04/07/2015 03/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONSULTORIO 2	BIMENSUAL	04/01/2015 05/04/2015 05/07/2015 04/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONSULTORIO 3	BIMENSUAL	04/01/2015 05/04/2015 05/07/2015 04/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONSULTORIO 4	BIMENSUAL	04/01/2015 05/04/2015 05/07/2015 04/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONSULTORIO 5	BIMENSUAL	10/01/2015 11/04/2015 11/07/2015 10/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONSULTORIO 6	BIMENSUAL	10/01/2015 11/04/2015 11/07/2015 10/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONSULTORIO 7	CUATRIMESTRAL	11/01/2015 12/04/2015 12/07/2015 11/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONSULTORIO 8	CUATRIMESTRAL	11/01/2015 12/04/2015 12/07/2015 11/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CITAS MEDICAS 1	TRIMESTRAL	06/01/2015 01/04/2015 01/07/2015 01/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CITAS MEDICAS 2	TRIMESTRAL	06/01/2015 01/04/2015 01/07/2015 01/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CITAS MEDICAS 3	TRIMESTRAL	06/01/2015 01/04/2015 01/07/2015 01/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CAJA DE CONSULTA EXTERNA I	TRIMESTRAL	08/01/2015 07/04/2015 07/07/2015 06/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CAJA DE CONSULTA EXTERNA II	TRIMESTRAL	08/01/2015 07/04/2015 07/07/2015 06/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CAJA DE CONSULTA EXTERNA II	TRIMESTRAL	08/01/2015 07/04/2015 07/07/2015 06/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	JEFE CONSULTA EXTERNA	TRIMESTRAL	13/01/2015 09/04/2015 09/07/2015 08/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	AUX CONSULTA EXTERNA	TRIMESTRAL	13/01/2015 09/04/2015 09/07/2015 08/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CAJA DE URGENCIAS	MENSUAL	15/01/2015 03/02/2015 03/03/2015 14/04/2015 05/05/2015 02/06/2015 14/07/2015 04/08/2015 01/09/2015 13/10/2015 03/11/2015 01/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	ADMISIONES	MENSUAL	15/01/2015 03/02/2015 03/03/2015 14/04/2015 05/05/2015 02/06/2015 14/07/2015 04/08/2015 01/09/2015 13/10/2015 03/11/2015 01/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	REFERENCIA	MENSUAL	15/01/2015 03/02/2015 03/03/2015 14/04/2015 05/05/2015 02/06/2015 14/07/2015 04/08/2015 01/09/2015 13/10/2015 03/11/2015 01/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	TRIAGE	MENSUAL	15/01/2015 03/02/2015 03/03/2015 14/04/2015 05/05/2015 02/06/2015 14/07/2015 04/08/2015 01/09/2015 13/10/2015 03/11/2015 01/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	URGENCIA C1	MENSUAL	20/01/2015 05/02/2015 05/03/2015 16/04/2015 07/05/2015 04/06/2015 16/07/2015 06/08/2015 03/09/2015 15/10/2015 05/11/2015 03/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	URGENCIA C2	MENSUAL	20/01/2015 05/02/2015 05/03/2015 16/04/2015 07/05/2015 04/06/2015 16/07/2015 06/08/2015 03/09/2015 15/10/2015 05/11/2015 03/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	URGENCIA C3	MENSUAL	20/01/2015 05/02/2015 05/03/2015 16/04/2015 07/05/2015 04/06/2015 16/07/2015 06/08/2015 03/09/2015 15/10/2015 05/11/2015 03/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	URGENCIA PROCED	MENSUAL	20/01/2015 05/02/2015 05/03/2015 16/04/2015 07/05/2015 04/06/2015 16/07/2015 06/08/2015 03/09/2015 15/10/2015 05/11/2015 03/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	URGENCIAS ENFERMERIA 1	MENSUAL	22/01/2015 10/02/2015 10/03/2015 21/04/2015 12/05/2015 09/06/2015 21/07/2015 11/08/2015 08/09/2015 20/10/2015 10/11/2015 08/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	URGENCIAS ENFERMERIA 2	MENSUAL	22/01/2015 10/02/2015 10/03/2015 21/04/2015 12/05/2015 09/06/2015 21/07/2015 11/08/2015 08/09/2015 20/10/2015 10/11/2015 08/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.

PC DE ESCRITORIO	URGENCIAS PEDIATRIA	MENSUAL	22/01/2015 10/02/2015 10/03/2015 21/04/2015 12/05/2015 09/06/2015 21/07/2015 11/08/2015 08/09/2015 20/10/2015 10/11/2015 08/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CIRUGIA 1	TRIMESTRAL	01/03/2015 07/06/2015 02/08/2015 01/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CIRUGIA 2	TRIMESTRAL	01/03/2015 07/06/2015 02/08/2015 01/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CIRUGIA 3	TRIMESTRAL	01/03/2015 07/06/2015 02/08/2015 01/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CIRUGIA 4	TRIMESTRAL	01/03/2015 07/06/2015 02/08/2015 01/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CIRUGIA 5	TRIMESTRAL	01/03/2015 07/06/2015 02/08/2015 01/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CIRUGIA 6	TRIMESTRAL	01/03/2015 07/06/2015 02/08/2015 01/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	MATERNIDAD CONSULTORIO	MENSUAL	23/01/2015 12/02/2015 12/03/2015 23/04/2015 14/05/2015 11/06/2015 23/07/2015 13/08/2015 10/09/2015 22/10/2015 12/11/2015 10/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	MATERNIDAD SALA PARTO	MENSUAL	23/01/2015 12/02/2015 12/03/2015 23/04/2015 14/05/2015 11/06/2015 23/07/2015 13/08/2015 10/09/2015 22/10/2015 12/11/2015 10/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	URGENCIAS PREPARTO	MENSUAL	23/01/2015 12/02/2015 12/03/2015 23/04/2015 14/05/2015 11/06/2015 23/07/2015 13/08/2015 10/09/2015 22/10/2015 12/11/2015 10/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	MATERNIDAD STAR 1	MENSUAL	26/01/2015 17/02/2015 17/03/2015 28/04/2015 19/05/2015 16/06/2015 28/07/2015 18/08/2015 15/09/2015 27/10/2015 17/11/2015 15/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	MATERNIDAD STAR 2	MENSUAL	26/01/2015 17/02/2015 17/03/2015 28/04/2015 19/05/2015 16/06/2015 28/07/2015 18/08/2015 15/09/2015 27/10/2015 17/11/2015 15/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	MATERNIDAD FACTURACION	MENSUAL	26/01/2015 17/02/2015 17/03/2015 28/04/2015 19/05/2015 16/06/2015 28/07/2015 18/08/2015 15/09/2015 27/10/2015 17/11/2015 15/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	HOSPITALIZACION MUJERES 1	MENSUAL	27/01/2015 19/02/2015 19/03/2015 29/03/2015 21/05/2015 18/06/2015 29/07/2015 20/08/2015 17/09/2015 28/10/2015 19/11/2015 17/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	HOSPITALIZACION MUJERES 2	MENSUAL	27/01/2015 19/02/2015 19/03/2015 29/03/2015 21/05/2015 18/06/2015 29/07/2015 20/08/2015 17/09/2015 28/10/2015 19/11/2015 17/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	HOSPITALIZACION MUJERES 3	MENSUAL	27/01/2015 19/02/2015 19/03/2015 29/03/2015 21/05/2015 18/06/2015 29/07/2015 20/08/2015 17/09/2015 28/10/2015 19/11/2015 17/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	HOSPITALIZACION HOMBRES 1	MENSUAL	28/01/2015 23/02/2015 24/03/2015 30/03/2015 25/05/2015 22/06/2015 30/07/2015 24/08/2015 21/09/2015 29/10/2015 23/11/2015 21/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	HOSPITALIZACION HOMBRES 2	MENSUAL	28/01/2015 23/02/2015 24/03/2015 30/03/2015 25/05/2015 22/06/2015 30/07/2015 24/08/2015 21/09/2015 29/10/2015 23/11/2015 21/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	HOSPITALIZACION HOMBRES 3	MENSUAL	28/01/2015 23/02/2015 24/03/2015 30/03/2015 25/05/2015 22/06/2015 30/07/2015 24/08/2015 21/09/2015 29/10/2015 23/11/2015 21/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	JEFE ENFERMERIA	MENSUAL	28/01/2015 23/02/2015 24/03/2015 30/03/2015 25/05/2015 22/06/2015 30/07/2015 24/08/2015 21/09/2015 29/10/2015 23/11/2015 21/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	PEDIATRIA STAR 1	MENSUAL	27/01/2015 19/02/2015 19/03/2015 29/03/2015 21/05/2015 18/06/2015 29/07/2015 20/08/2015 17/09/2015 28/10/2015 19/11/2015 17/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	PEDIATRIA STAR 2	MENSUAL	27/01/2015 19/02/2015 19/03/2015 29/03/2015 21/05/2015 18/06/2015 29/07/2015 20/08/2015 17/09/2015 28/10/2015 19/11/2015 17/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	PEDIATRIA CONSULTORIO	MENSUAL	27/01/2015 19/02/2015 19/03/2015 29/03/2015 21/05/2015 18/06/2015 29/07/2015 20/08/2015 17/09/2015 28/10/2015 19/11/2015 17/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	PEDIATRIA NEONATOS	MENSUAL	27/01/2015 19/02/2015 19/03/2015 29/03/2015 21/05/2015 18/06/2015 29/07/2015 20/08/2015 17/09/2015 28/10/2015 19/11/2015 17/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.

PC DE ESCRITORIO	FISIOTERAPIA	CUATRIMESTRAL	06/02/2015 05/06/2015 09/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	ECOGRAFIAS	CUATRIMESTRAL	06/02/2015 05/06/2015 09/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	FACTURACION PISO 1	TRIMESTRAL	11/02/2015 06/05/2015 05/08/2015 04/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	FACTURACION JEFE	TRIMESTRAL	11/02/2015 06/05/2015 05/08/2015 04/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	FACTURACION AUTORIZACION	TRIMESTRAL	11/02/2015 06/05/2015 05/08/2015 04/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	RADICACIONES	TRIMESTRAL	11/02/2015 06/05/2015 05/08/2015 04/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	LABORATORIO CLINICO JEFE	TRIMESTRAL	18/02/2015 18/05/2015 17/08/2015 18/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	LABORATORIO CLINICO SECRETARIA	TRIMESTRAL	18/02/2015 18/05/2015 17/08/2015 18/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	LABORATORIO PRUEBA 1	TRIMESTRAL	18/02/2015 18/05/2015 17/08/2015 18/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	LABORATORIO PRUEBA 2	TRIMESTRAL	18/02/2015 18/05/2015 17/08/2015 18/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	SERVICIO TRANSFUSIONAL	TRIMESTRAL	18/02/2015 18/05/2015 17/08/2015 18/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	SIAU	TRIMESTRAL	18/03/2015 15/06/2015 16/09/2015 16/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	SIAU	TRIMESTRAL	18/03/2015 15/06/2015 16/09/2015 16/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	AUDITORIA 1	TRIMESTRAL	13/03/2015 12/06/2015 11/09/2015 04/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	AUDITORIA 2	TRIMESTRAL	13/03/2015 12/06/2015 11/09/2015 04/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	AUDITORIA AUXILIAR	TRIMESTRAL	13/03/2015 12/06/2015 11/09/2015 04/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	AUDITORIA CUENTAS 1	TRIMESTRAL	13/03/2015 12/06/2015 11/09/2015 04/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	AUDITORIA CUENTAS 2	TRIMESTRAL	13/03/2015 12/06/2015 11/09/2015 04/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	FARMACIA JEFE	TRIMESTRAL	27/02/2015 27/05/2015 27/08/2015 27/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	FARMACIA ENTREGAS	BIMENSUAL	04/01/2015 05/04/2015 05/07/2015 04/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	FARMACIA ORDENES	TRIMESTRAL	27/02/2015 27/05/2015 27/08/2015 27/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CALIDAD	TRIMESTRAL	27/02/2015 27/05/2015 27/08/2015 27/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	ALMACEN JEFE	CUATRIMESTRAL	04/02/2015 13/05/2015 12/08/2015 11/011/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	ALMACEN AUXILIAR	CUATRIMESTRAL	04/02/2015 13/05/2015 12/08/2015 11/011/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	GESTION HUMANA JEFE	TRIMESTRAL	04/03/2015 03/06/2015 02/09/2015 02/09/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	GESTION HUMANA NOMINA	TRIMESTRAL	04/03/2015 03/06/2015 02/09/2015 02/09/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	GESTION HUMANA SECRETARIA	TRIMESTRAL	04/03/2015 03/06/2015 02/09/2015 02/09/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	COORDINACION MANTENIMIENTO	TRIMESTRAL	11/03/2015 10/06/2015 09/09/2015 09/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONTROL INTERNO	TRIMESTRAL	11/03/2015 10/06/2015 09/09/2015 09/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PORTATIL	GERENCIA	TRIMESTRAL	04/02/2015 13/05/2015 12/08/2015 11/011/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	GERENCIA SECRETARIA	TRIMESTRAL	04/02/2015 13/05/2015 12/08/2015 11/011/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	SUBGERENCIA ADMINISTRATIVA	TRIMESTRAL	25/02/2015 20/05/2015 19/08/2015 18/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	REVISORIA FISCAL	TRIMESTRAL	25/02/2015 20/05/2015 19/08/2015 18/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	PRESUPUESTO	TRIMESTRAL	25/02/2015 20/05/2015 19/08/2015 18/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	JURIDICA	TRIMESTRAL	09/03/2015 01/06/2015 07/09/2015 07/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	JURIDICA AUXILIAR	TRIMESTRAL	09/03/2015 01/06/2015 07/09/2015 07/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CARTERA JEFE	TRIMESTRAL	13/02/2015 08/05/2015 14/08/2015 06/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CARTERA AUX 1	TRIMESTRAL	13/02/2015 08/05/2015 14/08/2015 06/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CARTERA AUX 2	TRIMESTRAL	13/02/2015 08/05/2015 14/08/2015 06/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CARTERA AUX 3	TRIMESTRAL	20/02/2015 15/05/2015 21/08/2015 13/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CARTERA AUX 4	TRIMESTRAL	20/02/2015 15/05/2015 21/08/2015 13/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	COBRANZAS	TRIMESTRAL	20/02/2015 15/05/2015 21/08/2015 13/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONTABILIDAD	TRIMESTRAL	14/01/2015 08/04/2015 08/07/2015 21/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	CONTABILIDAD AUXILIAR	TRIMESTRAL	14/01/2015 08/04/2015 08/07/2015 21/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.

PC DE ESCRITORIO	TESORERIA	TRIMESTRAL	14/01/2015 08/04/2015 08/07/2015 21/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	ESTADISTICA JEFE	CUATRIMESTRAL	24/02/2015 26/05/2015 25/08/2015 24/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	ESTADISTICA AUXILIAR 1	CUATRIMESTRAL	24/02/2015 26/05/2015 25/08/2015 24/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	ESTADISTICA AUXILIAR 2	CUATRIMESTRAL	24/02/2015 26/05/2015 25/08/2015 24/11/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	SISTEMAS JEFE	CUATRIMESTRAL	11/03/2015 10/06/2015 09/09/2015 09/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	SISTEMAS AUXILIAR	CUATRIMESTRAL	11/03/2015 10/06/2015 09/09/2015 09/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	SERVIDOR DGH	CUATRIMESTRAL	09/02/2015 08/06/2015 05/10/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
PC DE ESCRITORIO	SERVIDOR SGD	CUATRIMESTRAL	09/02/2015 08/06/2015 05/10/2016	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
RACK	URGENCIA, ARCHIVO Y SISTEMA	CUATRIMESTRAL	09/02/2015 08/06/2015 05/10/2017	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.

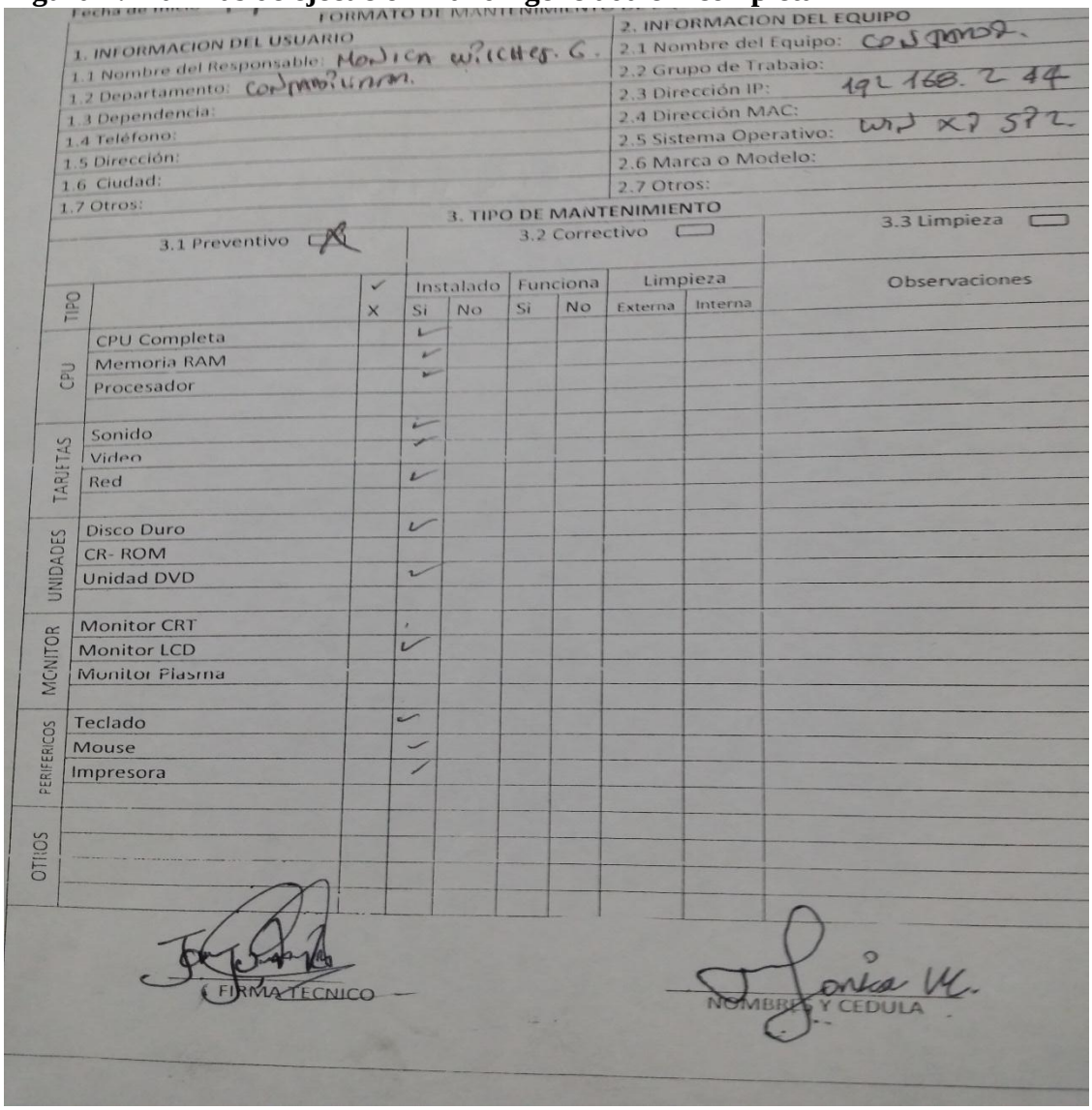
PLAN DE MANTENIMIENTO PREVENTIVO DE IMPRESORAS 2015

IMPRESORA LASER HP 1102W	ARCHIVO	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CONSULTORIO CON EXTERNA 1	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2016	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CONSULTORIO CON EXTERNA 2	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2017	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CONSULTORIO CON EXTERNA 3	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2018	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CONSULTORIO CON EXTERNA 4	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2019	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CONSULTORIO CON EXTERNA 5	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2020	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CONSULTORIO CON EXTERNA 6	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2021	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CONSULTORIO CON EXTERNA 7	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2022	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CONSULTORIO CON EXTERNA 8	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2023	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	JEFE CON EXTERNA	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2024	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CITAS 1	TRIMESTRAL	30/03/2015 30/06/2015 30/09/2015 16/12/2025	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	ADMISIONES	TRIMESTRAL	27/03/2015 24/06/2015 23/09/2015 18/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	REFERENCIA	TRIMESTRAL	27/03/2015 24/06/2015 23/09/2015 18/12/2016	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	TRIAGE	TRIMESTRAL	27/03/2015 24/06/2015 23/09/2015 18/12/2017	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	URGENCIAS CONSULTORIO 1	TRIMESTRAL	27/03/2015 24/06/2015 23/09/2015 18/12/2018	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	URGENCIAS CONSULTORIO 3	TRIMESTRAL	27/03/2015 24/06/2015 23/09/2015 18/12/2019	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	URGENCIAS STAR	TRIMESTRAL	27/03/2015 24/06/2015 23/09/2015 18/12/2020	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CIRUGIA 1	TRIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CIRUGIA 2	TRIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2016	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA TINATA EPSON L210	CIRUGIA 2	TRIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2017	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	MATERNIDAD CONSULTORIO	TRIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2017	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	MATERNIDAD STAR	TRIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2018	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	MUJERES STAR	MENSUAL	27/03/2015 25/06/2015 24/09/2015 09/12/2018	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	HOMBRES STAR	MENSUAL	27/03/2015 25/06/2015 24/09/2015 09/12/2018	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	PEDIATRIA CONSULTORIO	BIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2018	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA TINTA EPSON L200	LABORATORIO CLINICO JEFE	BIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2018	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación

IMPRESORA TINTA EPSON L210	LABORATORIO CLINICO ABACO	BIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2019	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	LABORATORIO CLINICO SECRETARIA	BIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2020	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA PUNTO LX 300	LABORATORIO CLINICO ABACO JUNIOR	BIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2021	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER XEROX 3117	SIAU	BIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2021	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	FARMACIA JEFE	BIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2021	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	FARMACIA AUXILIAR	BIMESTRAL	27/03/2015 25/06/2015 24/09/2015 09/12/2022	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	FISIOTERAPIA	BIMESTRAL	15/04/2015 26/08/2015 15/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	ECOGRAFIAS	BIMESTRAL	15/04/2015 26/08/2015 15/12/2016	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER SAMSUNG 2010	ALMACEN	BIMESTRAL	15/04/2015 26/08/2015 15/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	GESTION HUMANA	BIMESTRAL	15/04/2015 26/08/2015 15/12/2016	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER MULTIFUNCIONAL HP	GERENCIA	BIMESTRAL	30/03/2015 29/06/2015 29/09/2015 22/12/2015	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER MULTIFUNCIONAL HP	GERENCIA SECRETARIA	BIMESTRAL	30/03/2015 29/06/2015 29/09/2015 22/12/2016	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	SUBGERENCIA ADMINISTRATIVA	BIMESTRAL	30/03/2015 29/06/2015 29/09/2015 22/12/2017	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	PRESUPUESTO	BIMESTRAL	30/03/2015 29/06/2015 29/09/2015 22/12/2018	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	JURIDICA	BIMESTRAL	30/03/2015 29/06/2015 29/09/2015 22/12/2019	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	CARTERA	BIMESTRAL	30/03/2015 29/06/2015 29/09/2015 22/12/2020	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER MULTIFUNCIONAL HP	CONTABILIDAD	BIMESTRAL	30/03/2015 29/06/2015 29/09/2015 22/12/2021	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	ESTADISTICA	BIMESTRAL	30/03/2015 29/06/2015 29/09/2015 22/12/2022	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación
IMPRESORA LASER HP 1102W	SISTEMAS	BIMESTRAL	30/03/2015 29/06/2015 29/09/2015 22/12/2023	TECNICO DE SISTEMAS	Mantenimiento en General, Limpieza y lubricación

Fuente: Hospital

Figura 4. Planillas de ejecución mal diligenciada e incompleta



FORMATO DE MANTENIMIENTO

1. INFORMACION DEL USUARIO
1.1 Nombre del Responsable: Monica Wilches G.
1.2 Departamento: Compras
1.3 Dependencia:
1.4 Teléfono:
1.5 Dirección:
1.6 Ciudad:
1.7 Otros:

2. INFORMACION DEL EQUIPO
2.1 Nombre del Equipo: Computador
2.2 Grupo de Trabajo:
2.3 Dirección IP: 192.168.2.44
2.4 Dirección MAC:
2.5 Sistema Operativo: Win XP SP2.
2.6 Marca o Modelo:
2.7 Otros:

3. TIPO DE MANTENIMIENTO
3.1 Preventivo [X] 3.2 Correctivo [ ] 3.3 Limpieza [ ]

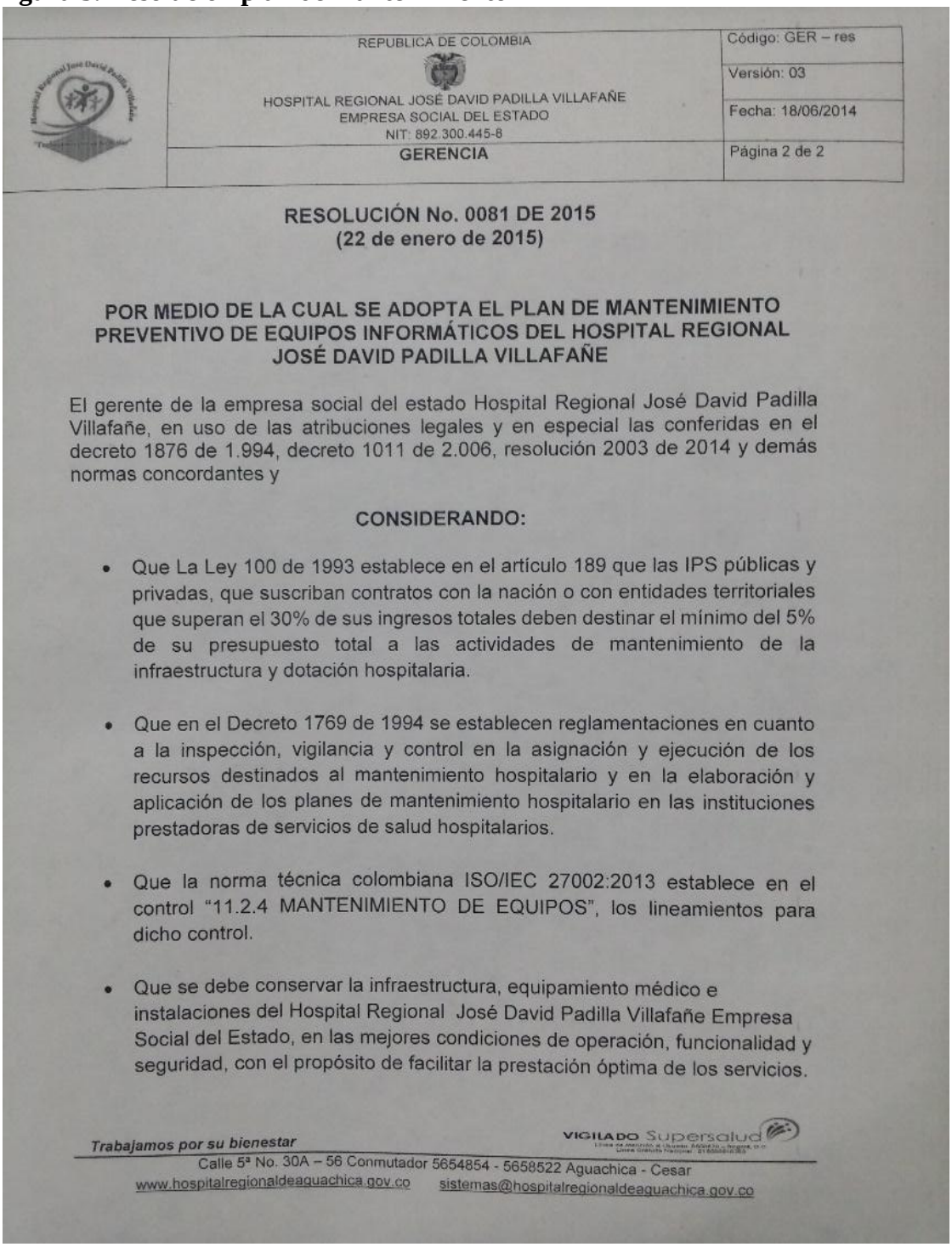
TIPO		✓ X	Instalado Si	Instalado No	Funciona Si	Funciona No	Limpieza Externa	Limpieza Interna	Observaciones
CPU	CPU Completa		✓						
	Memoria RAM		✓						
	Procesador		✓						
TARJETAS	Sonido		✓						
	Video		✓						
	Red		✓						
UNIDADES	Disco Duro		✓						
	CR- ROM								
	Unidad DVD		✓						
MONITOR	Monitor CRT		,						
	Monitor LCD		✓						
	Monitor Plasma								
PERIFERICOS	Teclado		✓						
	Mouse		✓						
	Impresora		/						
OTROS									

FIRMA TECNICO

NOMBRES Y CEDULA

Fuente: Hospital

Figura 5. Resolución plan de mantenimiento



	REPUBLICA DE COLOMBIA HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE EMPRESA SOCIAL DEL ESTADO NIT: 892.300.445-8 GERENCIA	Código: GER – res Versión: 03 Fecha: 18/06/2014 Página 2 de 2

RESOLUCIÓN No. 0081 DE 2015
(22 de enero de 2015)

POR MEDIO DE LA CUAL SE ADOPTA EL PLAN DE MANTENIMIENTO PREVENTIVO DE EQUIPOS INFORMÁTICOS DEL HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE

El gerente de la empresa social del estado Hospital Regional José David Padilla Villafañe, en uso de las atribuciones legales y en especial las conferidas en el decreto 1876 de 1.994, decreto 1011 de 2.006, resolución 2003 de 2014 y demás normas concordantes y

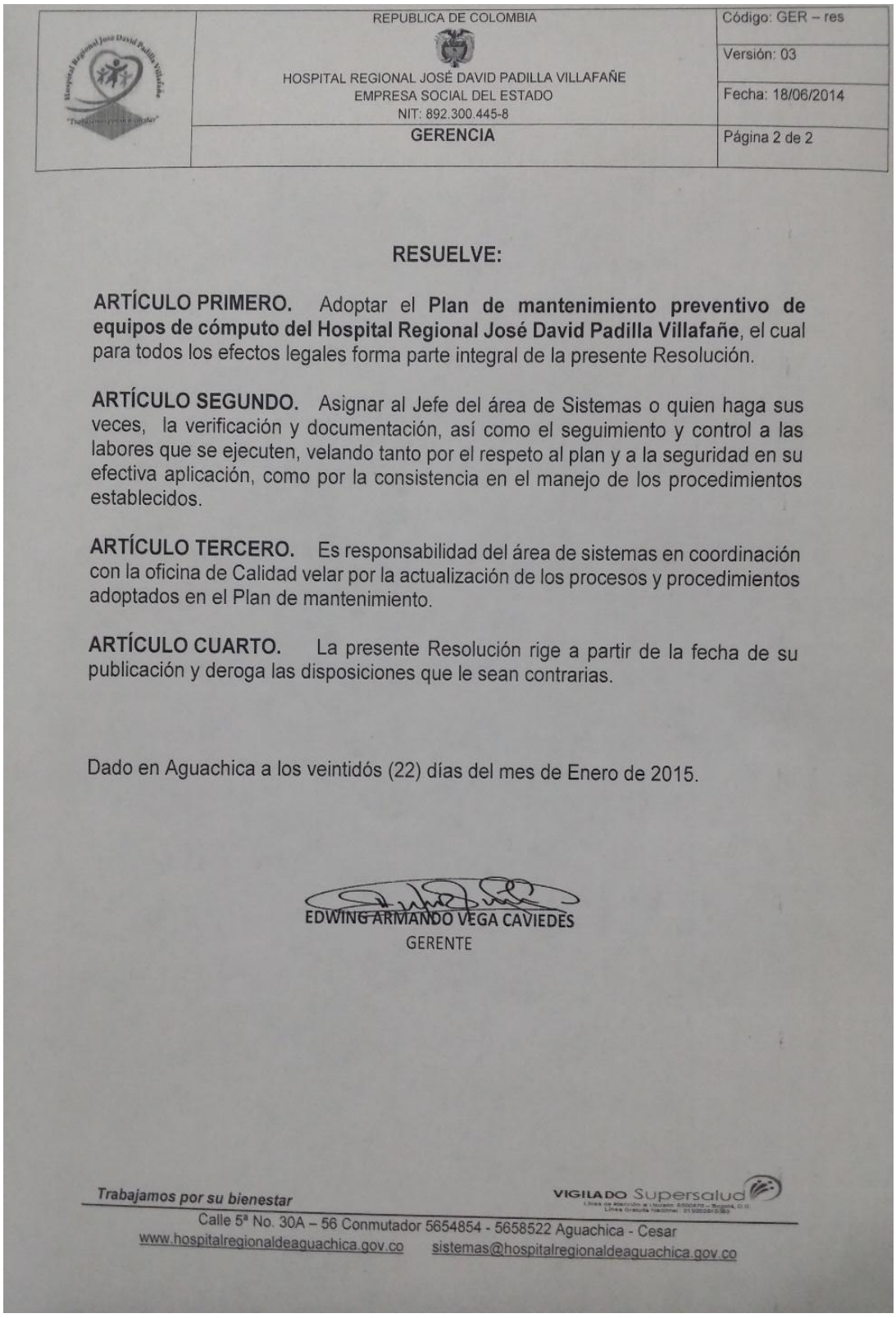
CONSIDERANDO:

- Que La Ley 100 de 1993 establece en el artículo 189 que las IPS públicas y privadas, que suscriban contratos con la nación o con entidades territoriales que superan el 30% de sus ingresos totales deben destinar el mínimo del 5% de su presupuesto total a las actividades de mantenimiento de la infraestructura y dotación hospitalaria.

- Que en el Decreto 1769 de 1994 se establecen reglamentaciones en cuanto a la inspección, vigilancia y control en la asignación y ejecución de los recursos destinados al mantenimiento hospitalario y en la elaboración y aplicación de los planes de mantenimiento hospitalario en las instituciones prestadoras de servicios de salud hospitalarios.

- Que la norma técnica colombiana ISO/IEC 27002:2013 establece en el control "11.2.4 MANTENIMIENTO DE EQUIPOS", los lineamientos para dicho control.

- Que se debe conservar la infraestructura, equipamiento médico e instalaciones del Hospital Regional José David Padilla Villafañe Empresa Social del Estado, en las mejores condiciones de operación, funcionalidad y seguridad, con el propósito de facilitar la prestación óptima de los servicios.



	REPUBLICA DE COLOMBIA	Código: GER – res
	HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE EMPRESA SOCIAL DEL ESTADO NIT: 892.300.445-8	Versión: 03 Fecha: 18/06/2014
	GERENCIA	Página 2 de 2

RESUELVE:

ARTÍCULO PRIMERO. Adoptar el **Plan de mantenimiento preventivo de equipos de cómputo del Hospital Regional José David Padilla Villafañe**, el cual para todos los efectos legales forma parte integral de la presente Resolución.

ARTÍCULO SEGUNDO. Asignar al Jefe del área de Sistemas o quien haga sus veces, la verificación y documentación, así como el seguimiento y control a las labores que se ejecuten, velando tanto por el respeto al plan y a la seguridad en su efectiva aplicación, como por la consistencia en el manejo de los procedimientos establecidos.

ARTÍCULO TERCERO. Es responsabilidad del área de sistemas en coordinación con la oficina de Calidad velar por la actualización de los procesos y procedimientos adoptados en el Plan de mantenimiento.

ARTÍCULO CUARTO. La presente Resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias.

Dado en Aguachica a los veintidós (22) días del mes de Enero de 2015.

EDWING ARMANDO VEGA CAVIEDES
GERENTE

Trabajamos por su bienestar

VIGILADO Supersalud

Calle 5ª No. 30A – 56 Conmutador 5654854 - 5658522 Aguachica - Cesar
www.hospitalregionaldeaguachica.gov.co sistemas@hospitalregionaldeaguachica.gov.co

Fuente: Hospital

Figura 6. Divulgación plan de mantenimiento

	REPUBLICA DE COLOMBIA HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE EMPRESA SOCIAL DEL ESTADO NIT: 892.300.445-8 **SISTEMAS**	Código: SIS – Act Versión: 02 Fecha: 18/06/2014 Página 1 de 1

Aguachica, 23 de enero de 2015

Licenciada
ELENA BAYETH
Hospitalización Hombres
Hospital regional José David padilla Villafañe E.S.E.

Cordial saludo,

La presente tiene como objetivo dar a conocer las fechas en las que quedo programado el mantenimiento preventivo de los equipos de cómputo ubicados en el área a su cargo, con el fin de que los equipos estén disponibles en los días estipulados para realizar el mantenimiento. Lo anterior para dar cumplimiento a la resolución No. 0081 del 22 Enero de 2015.

EQUIPO	FECHA	OBSERVACION
HOSPITALIZACION HOMBRES 1	28/01/2015 23/02/2015 24/03/2015 30/03/2015 25/05/2015 22/06/2015 30/07/2015 24/08/2015 21/09/2015 29/10/2015 23/11/2015 21/12/2015	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
HOSPITALIZACION HOMBRES 2	28/01/2015 23/02/2015 24/03/2015 30/03/2015 25/05/2015 22/06/2015 30/07/2015 24/08/2015 21/09/2015 29/10/2015 23/11/2015 21/12/2015	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.
HOSPITALIZACION HOMBRES 3	28/01/2015 23/02/2015 24/03/2015 30/03/2015 25/05/2015 22/06/2015 30/07/2015 24/08/2015 21/09/2015 29/10/2015 23/11/2015 21/12/2015	Mantenimiento en General, Limpieza, reconfiguración y escaneo de virus.

Atentamente,

GERARDO CESAR MOSQUERA QUINTERO
ASESOR DE SISTEMAS
HOSPITAL REGIONAL JOS DAVID PADILLA VILLAFAÑE

Trabajamos por su bienestar
VIGILADO Supersalud
Calle 5ª No. 30A – 56 Conmutador 5654854 - 5658522 Aguachica - Cesar
www.hospitalregionaldeaguachica.gov.co sistemas@hospitalregionaldeaguachica.gov.co

Fuente: Hospital

REPUBLICA DE COLOMBIA

HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE
EMPRESA SOCIAL DEL ESTADO
NIT: 892.300.445-8

REGISTRO DE ASISTENCIA A CAPACITACIÓN Y/O SOCIALIZACIÓN

Código: GHU- DGH- Fo -002	
Version:02	
Fecha de actualización: 08/07/2014	
Página 1 de 1	

TEMA DE CAPACITACION Y/O SOCIALIZACION	DIVULGACION PLAN DE MANTENIMIENTO EQUIPOS DE COMPUTO		
FECHA	23 - ENERO - 2015.	HORA	2:00 PM.
NOMBRE(S) DEL FUNCIONARIO RESPONSABLE	GERARDO CESAR MUSKUERA Q.		
CARGO	ASESOR DE SISTEMAS.		

NOMBRE DEL ASISTENTE	CEDULA	PROFESION	CARGO	CORREO ELECTRONICO	TELEFONO	FIRMA
Yadira Sanchez O.	37.332.274	Aux. contable	Facturadora	Yasan 20@hotmail.com	3116439435	
Gerardo Gomez	1'733.299.	Aux. Facturador	Facturador	munchogo31@hotmail.com	3186516787	
Diosa Gomez	26768325	Aux Factu	Factur-dor	diagojo.pl@Hotmail.com	3116553710	Diosa Gomez
Janiris Lemus Martinez	1065872365	Auxiliar F	Facturacion	janilemus@misena.ed.co	3133235581	
Ludys Sanchez M	49667 818	Auxiliar F	Aux. enfermeria	LudySanche@Hotmail.com.	3212366484	
Lucenith Santiago P	1065865735	Aux. Enf	Enfermera	lusucais10@hotmail.com	3128702353	
Jaeth Duarte	55221461	Aux. Fact	Facturadora	liceth ytu@ hotmail.com	3045867663	
Francisco Manosalva	1065862689	Aux. Autoriza	Aux Autorizadores	Francisco...@hotmail.com		
Zaida Cuan	26465093	Aux Facd	Aux Facd	Zoguerazdio@hotmail.com	3182416867	
Jhoson Reyes	96937736	Ins. Recaudo	Digitador	JACKSONRES@HOT-mail	3206994559	
Lina M.S.C	1064839558	Auxiliar	copias		3177324857	Lina M.S.C
Rosiris Dominguez	49651382	Facturadora	Facturadora	aidenydayana@hotmail.com	3107261434	

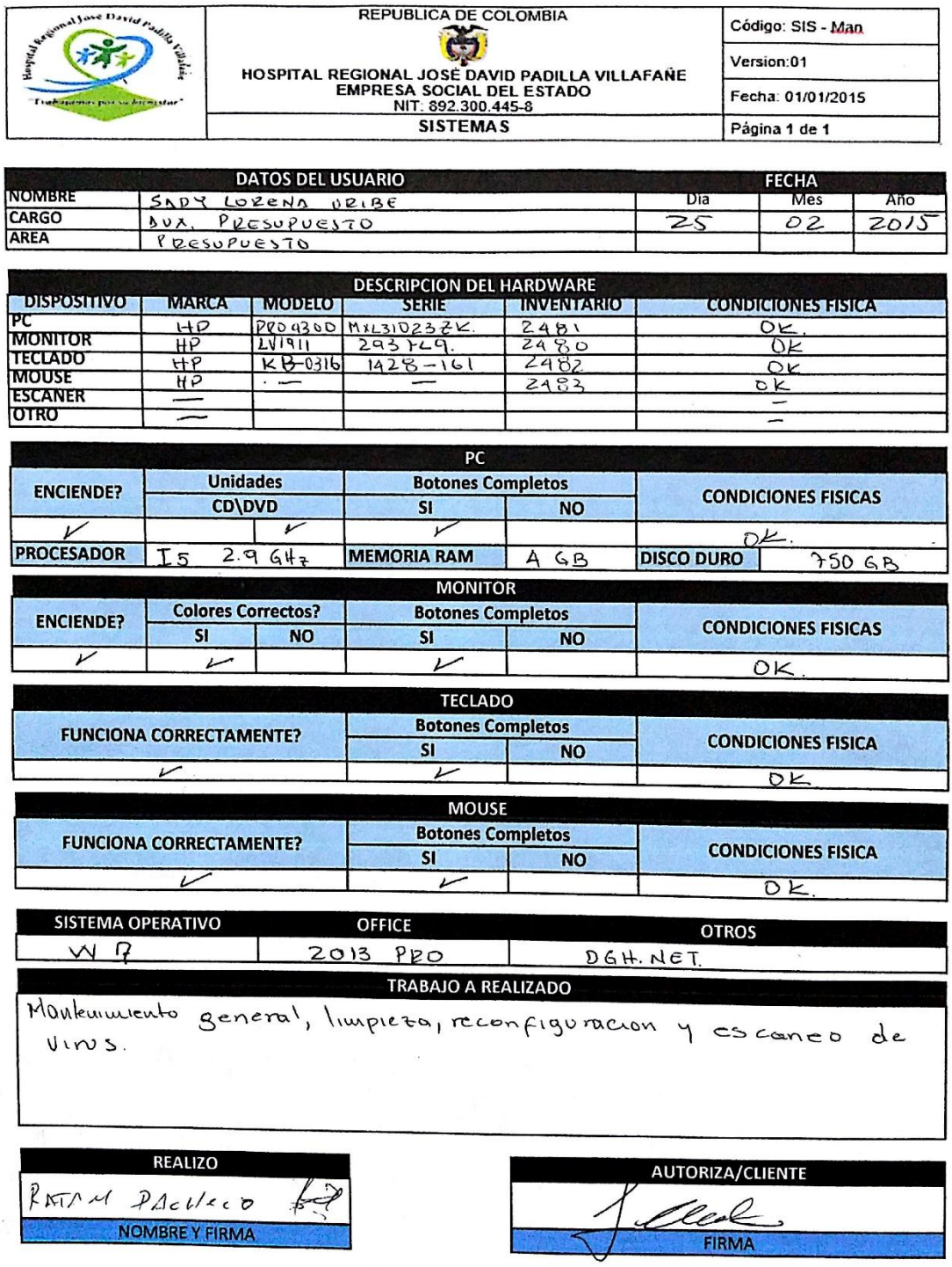
VIGILADO Supersalud

Trabajamos por su bienestar

Calle 5ª No. 30A – 56 Conmutador 5654854 - 5658522 Aguachica - Cesar
www.hospitalregionaldeaguachica.gov.co gestiónhumana@hospitalregionaldeaguachica.gov.co

Fuente: Autores del proyecto

Figura 7. Plantillas de ejecución correctamente diligenciadas



	REPUBLICA DE COLOMBIA	Código: SIS - Man
	HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE EMPRESA SOCIAL DEL ESTADO NIT: 892.300.445-8	Version:01
		Fecha: 01/01/2015
	SISTEMAS	Página 1 de 1

DATOS DEL USUARIO		FECHA		
		Dia	Mes	Año
NOMBRE	SADY LORENA URIBE	25	02	2015
CARGO	AUX. PRESUPUESTO			
AREA	PRESUPUESTO			

DESCRIPCION DEL HARDWARE

DISPOSITIVO	MARCA	MODELO	SERIE	INVENTARIO	CONDICIONES FISICA
PC	HP	PRO 4300	MXL3102332K.	2481	OK.
MONITOR	HP	LV1911	293 KL9.	2480	OK
TECLADO	HP	KB-0316	1428-161	2482	OK
MOUSE	HP	—	—	2483	OK
ESCANER	—				—
OTRO	—				—

PC

ENCIENDE?	Unidades		Botones Completos		CONDICIONES FISICAS	
	CD\DVD		SI	NO		
✓		✓	✓		OK.	
PROCESADOR	I5 2.9 GHz		MEMORIA RAM	4 GB	DISCO DURO	750 GB

MONITOR

ENCIENDE?	Colores Correctos?		Botones Completos		CONDICIONES FISICAS
	SI	NO	SI	NO	
✓	✓		✓		OK.

TECLADO

FUNCIONA CORRECTAMENTE?	Botones Completos		CONDICIONES FISICA
	SI	NO	
✓	✓		OK

MOUSE

FUNCIONA CORRECTAMENTE?	Botones Completos		CONDICIONES FISICA
	SI	NO	
✓	✓		OK.

SISTEMA OPERATIVO	OFFICE	OTROS
W 7	2013 PRO	DGH. NET.

TRABAJO A REALIZADO

Mantenimiento general, limpieza, reconfiguracion y escaneo de virus.

REALIZO	AUTORIZA/CLIENTE
RAFAEL PACHECO	
NOMBRE Y FIRMA	FIRMA

Fuente: Hospital

Figura 8. Actas de comparación plan de mantenimiento Vs plantilla de ejecución

	REPUBLICA DE COLOMBIA HOSPITAL REGIONAL JOSÉ DAVID PADILLA VILLAFAÑE EMPRESA SOCIAL DEL ESTADO NIT 892.300.445-8 **SISTEMAS**	Código: SIS – Act Versión: 02 Fecha: 18/06/2014 Página 1 de 1

ACTA DE REVISIÓN

PLAN DE MANTENIMIENTO HOSPITALARARIO DE EQUIPOS DE CÓMPUTO

En Aguachica, Departamento del Cesar, a los Cuatro (4) días del mes de marzo de Dos Mil Quince (2015), siendo las Cuatro de la tarde (04:00 p.m.) se reunieron los abajo firmantes para dar inicio a la revisión del plan de mantenimiento de los equipos de cómputo y las planillas de ejecución del mismo establecidos por el Hospital en la resolución Nro. 0080 de 2015 hallándose los siguientes hechos:

1. Se revisó la forma en que se divulgo el plan de mantenimiento a los empleados del Hospital, evidenciando los oficios dirigidos a las personas responsables del uso y cuidado de los equipos de cómputo, así como las panillas con los mismos firmantes reconociendo la existencia del plan de mantenimiento y la programación del mismo.

2. Se verificaron las planillas de ejecución de los mantenimientos realizados contra la programación establecida en el plan de mantenimiento y se halló que a tres (3) computadores no se les realizo el mantenimiento programado en el plan, estos son:

   - Archivo 2 programado para el día 04 de enero de 2015
   - Consultorio 5 programado para el día 10 de enero de 2015
   - Citas médicas 1 programado para el día 06 de enero de 2015.

   A lo cual el Técnico de sistemas indica que el personal que tenía en uso los equipos esos días no los facilito para la realización del mantenimiento programado.

3. Se dan directrices al técnico para que cuando sea imposible realizar el mantenimiento a los equipos por razones de fuerza mayor en los días programados, se reprogramen nuevas fechas lo más pronto posible con el fin de cumplir totalmente con el plan proyectado.

GERARDO CESAR MOSQUERA QUINTERO
Asesor de Sistemas

ARLEY RODRIGUEZ CAMACHO
Técnico de Sistemas

VIGILADO Supersalud

Fuente: Hospital

	REPUBLICA DE COLOMBIA HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE EMPRESA SOCIAL DEL ESTADO NIT: 892.300.445-8 **SISTEMAS**	Código: SIS – Act Versión: 02 Fecha: 18/06/2014 Página 1 de 1

ACTA DE REVISIÓN

PLAN DE MANTENIMIENTO HOSPITALARARIO DE EQUIPOS DE CÓMPUTO

En Aguachica, Departamento del Cesar, a los Cuatro (4) días del mes de mayo de Dos Mil Quince (2015), siendo las Tres y Veinticinco de la tarde (03:25 p.m.) se reunieron los abajo firmantes para dar inicio a la revisión del plan de mantenimiento de los equipos de cómputo y las planillas de ejecución del mismo establecidos por el Hospital en la resolución Nro. 0080 de 2015 hallándose los siguientes hechos:

1. Se verificaron las planillas de ejecución de los mantenimientos realizados contra la programación establecida en el plan de mantenimiento, así como el estado de los equipos atendidos y se comprobó la correcta ejecución del plan de mantenimiento y el diligenciamiento óptimo de las planillas de ejecución.

GERARDO CESAR MOSQUERA QUINTERO
Asesor de Sistemas

ARLEY RODRIGUEZ CAMACHO
Técnico de Sistemas

Fuente: Hospital

	REPUBLICA DE COLOMBIA HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE EMPRESA SOCIAL DEL ESTADO NIT 892 300 445-8 **SISTEMAS**	Código: SIS – Act Versión: 02 Fecha: 18/06/2014 Página 1 de 1

ACTA DE REVISIÓN

PLAN DE MANTENIMIENTO HOSPITALARARIO DE EQUIPOS DE CÓMPUTO

En Aguachica, Departamento del Cesar, a los Un (1) día del mes de Julio de Dos Mil Quince (2015), siendo las Ocho de la Mañana (08:00 a.m.) se reunieron los abajo firmantes para dar inicio a la revisión del plan de mantenimiento de los equipos de cómputo y las planillas de ejecución del mismo establecidos por el Hospital en la Resolución Nro. 0080 de 2015 hallándose los siguientes hechos:

1. Se verificaron las planillas de ejecución de los mantenimientos realizados contra la programación establecida en el plan de mantenimiento, así como el estado de los equipos atendidos y se comprobó la correcta ejecución del plan de mantenimiento y el diligenciamiento óptimo de las planillas de ejecución.

GERARDO CESAR MOSQUERA QUINTERO
Asesor de Sistemas

ARLEY RODRIGUEZ CAMACHO
Técnico de Sistemas

Fuente: Hospital

	REPUBLICA DE COLOMBIA HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE EMPRESA SOCIAL DEL ESTADO NIT 892 300 445-8 **SISTEMAS**	Código: SIS – Act Versión: 02 Fecha: 18/06/2014 Página 1 de 1

ACTA DE REVISIÓN

PLAN DE MANTENIMIENTO HOSPITALARARIO DE EQUIPOS DE CÓMPUTO

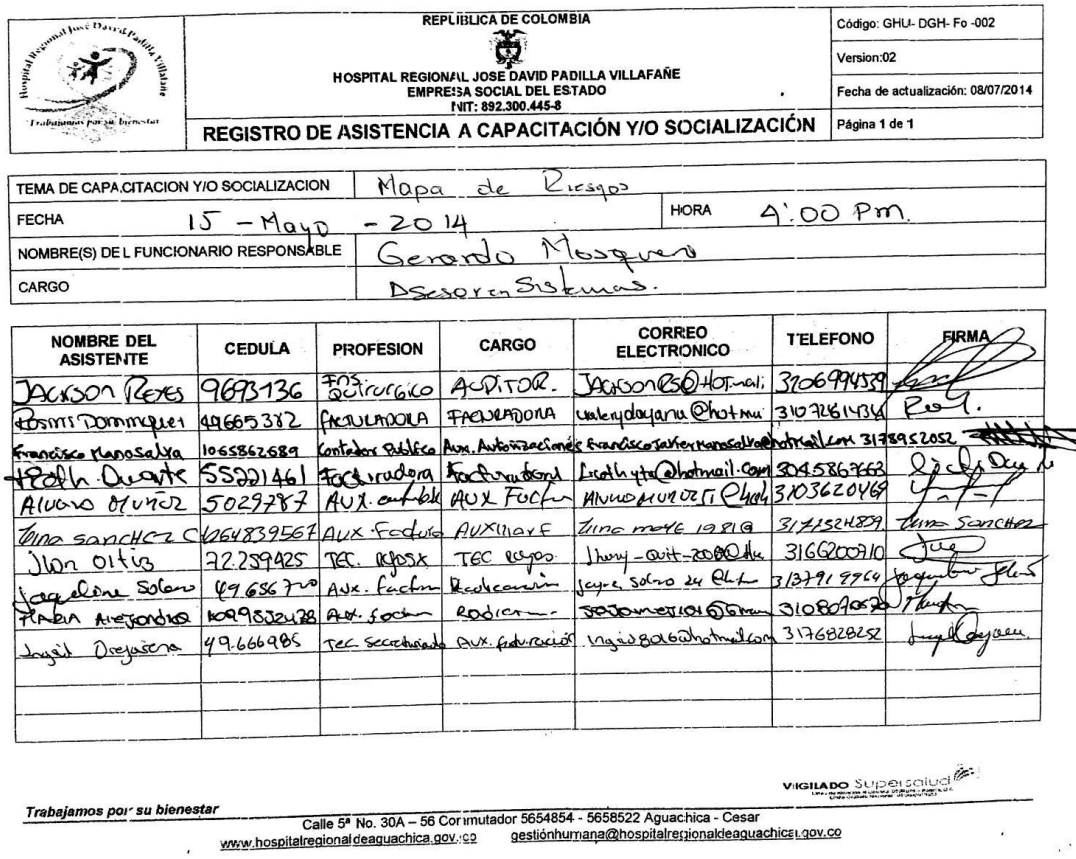
En Aguachica, Departamento del Cesar, a los Un (1) día del mes de Septiembre de Dos Mil Quince (2015), siendo las Ocho y Veintitrés de la Mañana (08:23 a.m.) se reunieron los abajo firmantes para dar inicio a la revisión del plan de mantenimiento de los equipos de cómputo y las planillas de ejecución del mismo establecidos por el Hospital en la Resolución Nro. 0080 de 2015 hallándose los siguientes hechos:

1. Se verificaron las planillas de ejecución de los mantenimientos realizados contra la programación establecida en el plan de mantenimiento, así como el estado de los equipos atendidos y se comprobó la correcta ejecución del plan de mantenimiento y el diligenciamiento óptimo de las planillas de ejecución.

GERARDO CESAR MOSQUERA QUINTERO
Asesor de Sistemas

ARLEY RODRIGUEZ CAMACHO
Técnico de Sistemas

Fuente: Hospital



REPUBLICA DE COLOMBIA

HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE
EMPRESA SOCIAL DEL ESTADO
NIT: 892.300.445-8

Código: GHU- DGH- Fo -002	
Version:02	
Fecha de actualización: 08/07/2014	
Página 1 de 1	

REGISTRO DE ASISTENCIA A CAPACITACIÓN Y/O SOCIALIZACIÓN

TEMA DE CAPACITACION Y/O SOCIALIZACION	Mapa de Riesgos
FECHA	15 - Mayo - 2014
HORA	4:00 Pm.
NOMBRE(S) DE L FUNCIONARIO RESPONSABLE	Gerardo Mosquera
CARGO	Asesor en Sistemas.

NOMBRE DEL ASISTENTE	CEDULA	PROFESION	CARGO	CORREO ELECTRONICO	TELEFONO	FIRMA
JACKSON REYES	9693136	Fis Quirurgico	AUDITOR.	JACKSON1650@Hotmail.	3106994559	
ROSMIS DOMINGUEZ	49665382	FACTURADORA	FACTURADORA	valeydayana@hotmail	3107261434	
Francisco Manosalva	1065862689	Contador Publico	Aux. Autorizaciones	franciscoxavier.manosalva@hotmail.com	3178952052	
Heath Duarte	55221461	Facturadora	Facturadora	Leath.ytz@hotmail.com	3045867663	
Alvaro Olivos	5029787	AUX. contable	AUX Factu	Alvaroolivos1@hotmail.com	3103620469	
Zima Sanchez C	1064839567	AUX. Factura	AUXILIAR F	Zima.meye.1981@	3115248859	
Jhon Ortiz	72.259425	TEC. RAYOS X	TEC Rayos	Jhony-ortiz-2008@hotmail	3166200910	
Jaqueline Solano	49.686.700	Aux. Factur	Recepcionis	jaqueline.solano.24@hotmail	3137918764	
Flabia Avendaño	1099532428	Aux. Factur	Recepcion	[illegible]	3108[illegible]	
Ingrid Ovejasera	49.666985	Tec. Secretariado	Aux. Facturación	Ingrid8016@hotmail.com	3176828252	

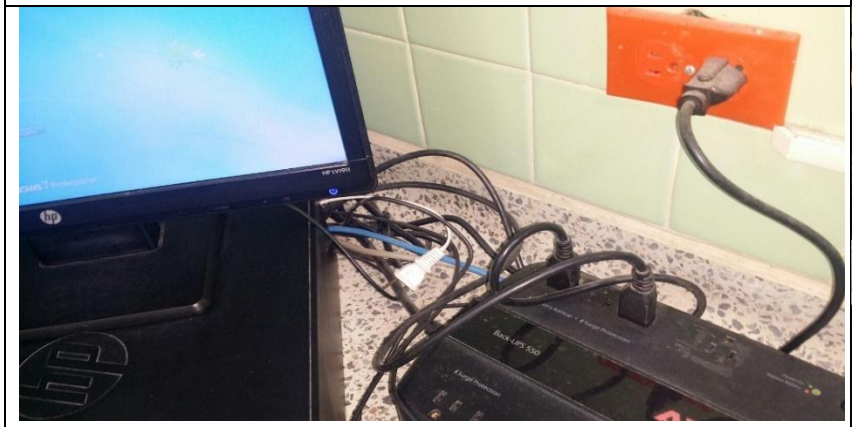
VIGILADO Supersalud

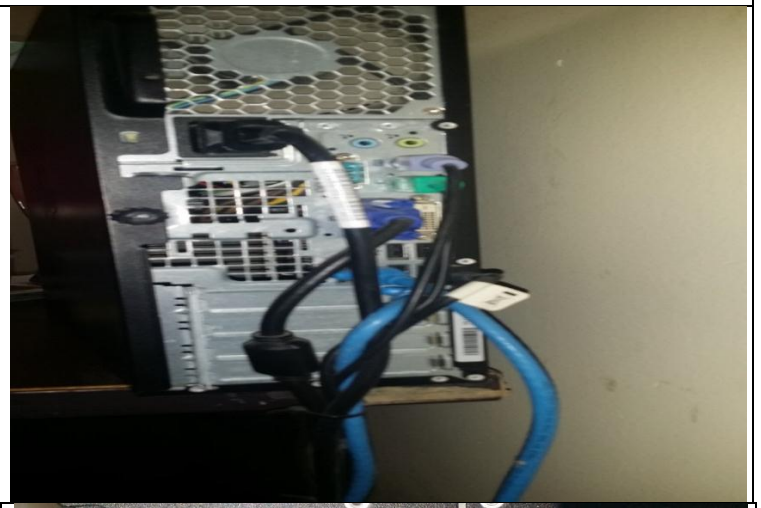
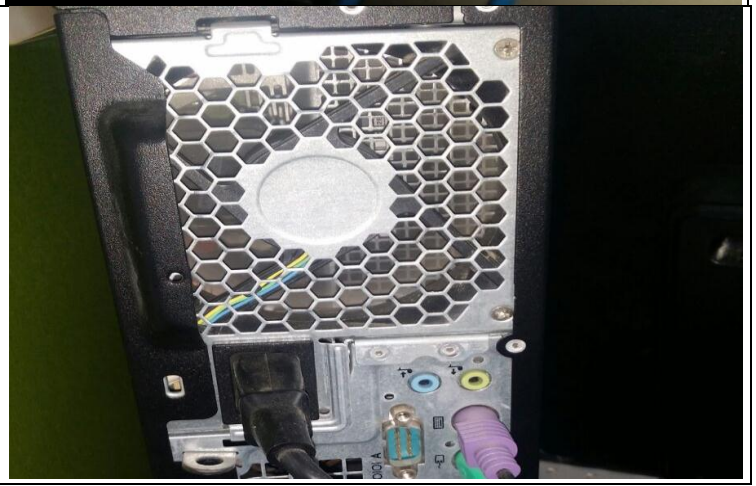
Trabajamos por su bienestar

Calle 5ª No. 30A – 56 Conmutador 5654854 - 5658522 Aguachica - Cesar
www.hospitalregionaldeaguachica.gov.co gestionhumana@hospitalregionaldeaguachica.gov.co

Fuente: Hospital

Fotografías equipos antes y después de la adopción de políticas y plan de mejoramiento.

CUADRO COMPARATIVO DE EQUIPOS DE COMPUTO	
ANTES	DESPUES
	
	

ANTES	DESPUES
	
	

Fuente: Autores del proyecto

Encuesta

ENCUESTA DIRIGIDA A LOS EMPLEADOS DEL HOSPITAL REGIONAL JOSE PADILLA VILLAFAÑE PARA DEMOSTRAR EFECTIVIDAD DE POLITICAS DE SEGURIDAD Y PLAN DE MOJORAMIENTO ADOPTADO

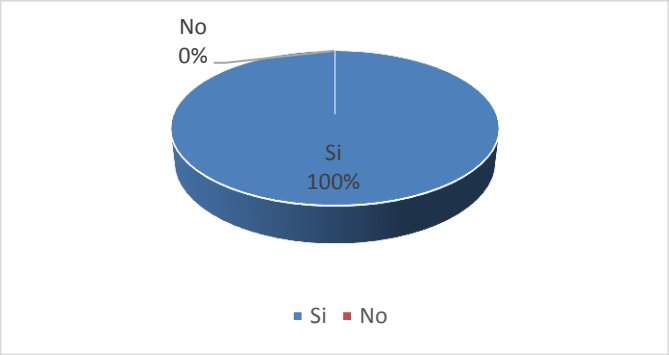
Pregunta No. 1 ¿Se le dio a conocer con anterioridad las fechas en las que se realizaría mantenimiento preventivo a los equipos de cómputo a su cargo?

TABLA 8. Conocimiento de fechas de mantenimientos

RESPUESTA	CANTIDAD	PORCENTAJE
Si	137	100%
No	0	0%
Total	137	100%

Fuente: Autores del proyecto

Figura 9. Conocimientos de las fechas de los mantenimientos preventivos de los equipos de cómputo.



Fuente: Autores del proyecto

Interpretación: La grafica muestra que luego de la implementación y socialización de las políticas de seguridad, así como la adopción del el plan de mejoramiento, los empleados manifestaron en su totalidad conocer las fechas en las cuales sus equipos de cómputo tendrían mantenimientos preventivos y así poder programar sus actividades con tiempo.

Pregunta no. 2¿Está satisfecho con los mantenimientos realizados a los equipos de cómputo a su cargo?

Tabla 9. Estado de satisfacción con los mantenimientos realizados

RESPUESTA	CANTIDAD	PORCENTAJE
Si	137	100%
No	0	0%
Total	137	100%

Fuente: Autores del proyecto

Figura 10. Conformidad con los mantenimientos realizados

Fuente: Autores del proyecto

Interpretación: La grafica muestra que la totalidad del personal encuestado, está satisfecho con los mantenimientos realizados a los equipos de cómputo a su cargo, demostrando así la efectividad de las políticas y plan de mejoramiento adoptados

TABLA 10 Cuadro comparativo encuesta anterior Vs Encuesta actual

Pregunta 1 ¿Se le dio a conocer con anterioridad las fechas en las que se realizaría mantenimiento preventivo a los equipos de cómputo a su cargo?

Pregunta 2 ¿Está satisfecho con los mantenimientos realizados a los equipos de cómputo a su cargo?

ENCUESTA	Pregunta 1		Pregunta 2	
	Si	NO	SI	NO
Anterior	7	130	68	69
Actual	137	0	137	0

Fuente: Autores del proyecto

Del anterior cuadro puede resaltarse que el total de los empleados encuestados aseguraron encontrarse satisfechos con los mantenimientos realizados a sus equipos en cuanto al conocimiento y cumplimiento de las fechas programadas y el rendimiento de los equipos luego de las actividades realizadas, demostrando con esto la efectividad en la adopción tanto de las políticas como del plan de mejoramiento.

CONCLUSIONES

La auditoría realizada en el Hospital Regional José David Padilla Villafañe E.S.E., permitió recolectar información que sirvió de insumo para la realización de mapas de riesgos y cuadros comparativos, estableciendo de esta manera la situación actual en la que se encontraba el hospital.

Si bien el hospital contaba con controles y políticas establecidos, estos no estaban estructurados de acurdo a ningún estándar o modelo de Gestión de la Seguridad de la Información, razón por la cual se definen y documentan nuevas políticas de seguridad física y del ambiente para dar protección a lo relacionado con este dominio y así contribuir con mecanismos que ayuden a garantizar la custodia de la información.

Por otra parte, se entregó un plan de mejora con mecanismos optimizados, que de ser adoptado por el hospital permitirá que este pueda gestionar mejor los riesgos encontrados.

Se concluye que la gestión de la seguridad de información no es un tema que pueda tratarse con un solo dominio debido a que la interrelación entre todos los dominios de la norma son los que permitirán una correcta seguridad de la información.

RECOMENDACIONES

En aras de una óptima protección de la información del Hospital, se recomienda la elaboración de las políticas de seguridad de la información, teniendo en cuenta el total de los dominios de la norma ISO/IEC 27002.

Lo anterior debido a que la protección de la información no puede garantizarse cubriendo un solo dominio de la norma.

Posterior a esto se deberá oficializar mediante resolución de Gerencia, publicado y divulgado con los empleados y todo el personal que se relacione con dichas políticas, así mismo deberán evaluarse periódicamente para verificar la eficacia y garantizar la continuidad de las mismas.

BIBLIOGRAFÍA

GIL PECHUÁN, Ignacio. Sistemas y Tecnologías de la Información para la Gestión. Madrid, McGraw-Hill, 1997.

ANGARITA LÓPEZ, Liseth Tatiana. Diseño del plan de gestión de seguridad de la información para controlar el acceso a las áreas restringidas de la empresa Ingepec LTDA en la ciudad de Ocaña: Tesis de grado para especialización en auditoría de sistemas, 2014.

ALIAGA FLORES, Luis Carlos. Diseño de un sistema de gestión de seguridad de la información para un instituto educativo: Tesis de grado, Pontificia Universidad Católica del Perú, 2013.

ISCALA TOBITO, Narcy Auristela. Diseño de un protocolo de seguridad de la información del área financiera de la secretaria de educación departamental de Norte de Santander Ocaña: Tesis de grado para especialización en auditoría de sistemas, 2014.

HERNÁNDEZ PINTO, María Gabriela. Tesis Diseño de un Plan Estratégico de Seguridad de Información en una empresa del sector comercial, Escuela Superior Politécnica del Litoral.2006. Guayaquil, Ecuador.

REYES CASADIEGOS, María Teresa. Álvarez Cabrales, Andru. Tesis Diseño de Políticas de Seguridad de la Información para la Oficina de Archivo y Correspondencia de la Universidad Francisco de Paula Santander Ocaña. Universidad Francisco de Paula Santander Ocaña. 2013. Colombia

ALONSO TAMAYO ÁLZATE. Auditoria de sistema una visión. Primera edición. Manizales. 2003.

GÓMEZ VIEITES, Álvaro., Enciclopedia de la Seguridad Informática, Alfa omega Grupo editor, México, Primera Edición, 2007.

NTC ISO/IEC 5411 - 1:2006. Tecnología de la información. Técnicas de seguridad. Gestión de la seguridad de la tecnología de la información y las comunicaciones. Parte 1: Conceptos y modelos para la gestión de la tecnología de la información y las comunicaciones (ISO/IEC 13335-1:2004).

Norma Técnica NTC ISO/IEC 27001:201, Sistemas de Gestión de la Seguridad de la Información (SGSI).

DALTABUIT GODAS Enrique, VÁSQUEZ José de Jesús, La seguridad de la información". Limusa Noriega Editores, 2007. p. 215.

NIMA RAMOS Jonathan D, Guía para la elaboración de planes de recuperación para sistemas de información empresarial y de negocios, Universidad de Plura, 2014.

DALTABUIT GODAS Enrique, VÁSQUEZ José de Jesús, La seguridad de la información". Limusa Noriega Editores, 2007. p. 26

DALTABUIT GODAS Enrique, VÁSQUEZ José de Jesús, La seguridad de la información". Limusa Noriega Editores, 2007. p. 221.

CONSTITUCIÓN POLÍTICA DE COLOMBIA, Ley Estatutaria 1581 de 2012, reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

TÉCNICAS Y CERTIFICACIÓN. Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. Bogotá D.C.: ICONTEC, 2007.NTC ISO/IEC 27002.

ECHENIQUE GARCÍA, José Antonio. Auditoría en informática. 2da edición. Bogotá: McGraw Hill, 2004. 300p.

NORMA ISO/IEC 27002: 2013

ICONTEC, 2013. NTC ISO/IEC 27001. INSTITUTO COLOMBIANO DE NORMAS.

CYBERGRAFIA

VEGA BRICEÑO, Edgar Armando. Los sistemas de información y su importancia para las organizaciones y empresas. [En línea]. [Citado el 03 octubre de 2014]. Disponible en internet.
<http://www.gestiopolis.com/Canales4/mkt/simparalas.htm>

MONTENEGRO, Luis. Artículo: Seguridad de la Información: Más que una actitud, un estilo de vida. [En línea]. [Citado el 05 Febrero de 2015]. Disponible en internet.
http://www.microsoft.com/conosur/technet/articulos/seguridadinfo/

HJDPV (2015) Hospital Regional José David Padilla Villafañe de Aguachica, Cesar.
http://www.hospitalregionaldeaguachica.gov.co/

ANEXOS

AUDITORIA DE SISTEMAS REALIZADA A LA SEGURIDAD FÍSICA Y AMBIENTAL EN EL HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE ESE. BASADOS EN EL ESTÁNDAR INTERNACIONAL ISO/IEC 27002:2013

En harás de proteger la seguridad informática del Hospital, algunas de las situaciones encontradas fueron alteradas, afirmando de esta manera que lo aquí plasmado no refleja verazmente la situación del Hospital.

Aguachica 17 de Mayo de 2014

DOCTOR
EDWING ARMANDO VEGA CAVIEDES
GERENTE
Hospital Regional De Aguachica José David Padilla Villafañe E. S. D

Cordial saludo,

El objetivo del ejercicio consistió en evaluar el cumplimiento de las políticas de seguridad según el estándar ISO 27002 de 2013 en un periodo comprendido del 14 de abril de 2014 al 17 de mayo de 2014.

De los resultados obtenidos durante la evaluación me permito informarle a Usted, los siguientes hechos evidenciados:

- Falta el documento que soporte la divulgación de políticas.
- Acceso no autorizado a recursos informáticos y áreas restringidas.
- El hospital no cuenta con mecanismos de advertencia (alarmas, sensores) que contribuyan a una rápida reacción frente a los factores externos causantes de desastres.
- Falta el documento que demuestre la divulgación de plan de mantenimiento preventivo y el seguimiento de la ejecución del mismo.

Esperamos que la información proporcionada sea de utilidad para el mejoramiento continuo de la organización que usted dirige.

Gracias por la atención recibida.

JORGE ARMANDO SARAVIA ALVERNIA

LIDER AUDITOR

1. HOJA DE IDENTIFICACIÓN

<table>
<tr><td colspan="3"> 
CSI AUDIS
Consultores de Sistemas de Información - Auditores de Sistemas</td></tr>
<tr><td colspan="3">NUMERO DE LA AUDITORIA A-005 2014
TIPO C
OFICIO DE ORDEN DE AUDITORIA 001
FECHA DE INICIO: Agosto 22 de 2014
FECHA DE TERMINO: Septiembre 02 de 2014</td></tr>
<tr><td colspan="3">EMPRESA A AUDITAR HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE</td></tr>
<tr><td rowspan="4">AUDITORES RESPONSABLES</td><td>NOMBRE</td><td>INICIALES</td></tr>
<tr><td>GERARDO CESAR MOSQUERA QUINTERO</td><td>GM</td></tr>
<tr><td>JORGE ARMANDO SARAVIA ALVERNIA</td><td>JS</td></tr>
<tr><td>JOSÉ JULIÁN PACHECO PÉREZ</td><td>JP</td></tr>
<tr><td colspan="2">DOCUMENTO PREPARADO POR:</td><td>GERARDO CESAR MOSQUERA QUINTERO
JORGE ARMANDO SARAVIA ALVERNIA
JOSÉ JULIÁN PACHECO PÉREZ</td></tr>
</table>

Fuente: Equipo auditor.

2. ÍNDICE DE CONTENIDO DE LOS PAPELES DE TRABAJO

CSI AUDIS

Consultores de Sistemas de Información - Auditores de Sistem

EMPRESA A AUDITAR	HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE

ARCHIVOS PERMANENTES	
CONTENIDO	**NOMENCLATURA**
Misión	AP1 – 1/1
Visión	AP2 – 1/1
Principios corporativos	AP3 – 1/1
Valores corporativos	AP4 – 1/2
Organigrama de la organización	AP5 – 1/1
Organigrama del área de sistemas	AP6 – 1/1
Normas y políticas de seguridad de la información	AP7 –1/ 1
Inventario de hardware	AP8– 1/1

ARCHIVOS CORRIENTES	
CONTENIDO	**NOMENCLATURA**
Programa general	AC1 – 1/2
Situaciones encontradas	AC2 – 1/1
Encuesta	AC3 – ½
Listas de chequeo	AC4 – 1/6
Matriz de riesgos	AC5 – 1/1
Pruebas de cumplimiento	AC6 – 1/1
Pruebas sustantivas	AC7– 1/1
Informe	AC8 – 1/1

DOCUMENTO PREPARADO POR:	GERARDO CESAR MOSQUERA QUINTERO JORGE ARMANDO SARAVIA ALVERNIA JOSÉ JULIÁN PACHECO PÉREZ

2.1 ARCHIVOS PERMANENTES

2.1.1 Misión

 CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas	**AP1 – 1/1**
EMPRESA A AUDITAR HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE	
MISIÓN	
Nuestro compromiso es la excelente prestación de servicios de salud en la región, participando en el progreso social, científico, económico y docente asistencial de la misma, generando satisfacción a nuestros clientes internos y externos con tecnología de punta y talento humano altamente calificado.	
DOCUMENTO PREPARADO POR:	GERARDO CESAR MOSQUERA QUINTERO JORGE ARMANDO SARAVIA ALVERNIA JOSÉ JULIÁN PACHECO PÉREZ

FUENTE: HOSPITAL

2.1.2 Visión

 CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas	**AP2 – 1/1**
EMPRESA A AUDITAR HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE	
VISIÓN	
En el 2016 seremos líderes en la atención de salud de II y III nivel de complejidad, con moderna infraestructura, excelente clima organizacional, calidad y tecnología apoyados en talento humano comprometido, beneficiando a los usuarios de Aguachica y su área de influencia.	
DOCUMENTO PREPARADO POR:	GERARDO CESAR MOSQUERA QUINTERO JORGE ARMANDO SARAVIA ALVERNIA JOSÉ JULIÁN PACHECO PÉREZ

FUENTE: HOSPITAL

2.1.3 Principios corporativos

CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas	**AP3 – 1/1**

EMPRESA A AUDITAR HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE

PRINCIPIOS CORPORATIVOS

1. **EFECTIVIDAD EN LA PRESTACIÓN DEL SERVICIO:** Ofrecemos los mejores servicios técnico-científicos a la comunidad, satisfaciendo las necesidades de nuestros usuarios.

2. **RESPONSABILIDAD SOCIAL:** Garantizamos a nuestros usuarios atención en salud, independiente de su condición económica y social.

3. **EDUCACIÓN**: Nuestra entidad participa activamente en la formación del talento humano, buscando una mejor competencia y desempeño.

4. **OPORTUNIDAD:** Asegurar que nuestros usuarios reciban servicios óptimos y a tiempo.

5. **LIDERAZGO:** Nuestra organización trabaja activamente para lograr el posicionamiento como los mejores en prestación de servicios de salud en la región.

6. **HUMANIZACIÓN:** Trabajamos por la dignificación de la vida.

7. **ECONOMÍA:** Nos orientamos hacia una política de sana austeridad y mesura en el gasto público, hacia un equilibrio conveniente y necesario en la inversión, garantizando así la debida proporcionalidad y conformidad de resultados en los términos costo-beneficios.

DOCUMENTO PREPARADO POR:	GERARDO CESAR MOSQUERA QUINTERO JORGE ARMANDO SARAVIA ALVERNIA JOSÉ JULIÁN PACHECO PÉREZ

FUENTE: HOSPITAL

2.1.4 Valores corporativos

 CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas	**AP4 – ½**
EMPRESA A AUDITAR	HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE
VALORES CORPORATIVOS	
1. **Responsabilidad:** Los funcionarios del H.J.D.P.V. deben caracterizarse por cumplir sus funciones y prestar los servicios asignados oportunamente con los recursos propios del cargo que desempeña. 2. **Compromiso:** Los funcionarios asumen cada una de sus obligaciones tanto en sus aciertos como en sus fallas, buscando el mejoramiento continuo y la calidad en los servicios prestados. 3. **Honestidad:** Los funcionarios se comportan y expresan con coherencia y sinceridad, respetando la verdad y justicia en cada una de sus actuaciones. 4. **Solidaridad:** Trabajamos en pro de la igualdad, fraternidad, ayuda mutua y la practicamos sin distinción de credo, sexo, raza, nacionalidad o afiliación política, cuya finalidad es el ser humano necesitado. 5. **Confianza**: Actuamos adecuadamente, generando seguridad en el deber ser y el hacer que garantizan el cumplimiento de nuestra misión. 6. **Transparencia:** Los funcionarios del HJDPV se caracterizan por prestar los servicios acordes a su plan de cargos, de manera clara, ética y moral en cada uno de sus procesos liderados, los cuales se reflejaran en la calidad de la atención brindada. 7. **Respeto:** Los trabajadores del HJDPV se caracterizan por prestar sus servicios basados en la dignificación del ser humano, la preservación de la vida, la tolerancia y convivencia pacífica en toda la región. 8. **Prudencia:** Nuestros funcionarios estarán dispuestos a reflexionar y considerar los efectos que pueden ocasionar sus palabras y acciones, dando como resultado el actuar correcto en cualquier circunstancia.	
DOCUMENTO PREPARADO POR:	GERARDO CESAR MOSQUERA QUINTERO JORGE ARMANDO SARAVIA ALVERNIA JOSÉ JULIÁN PACHECO PÉREZ

CSI AUDIS Consultores de Sistemas de Información - Auditores	**AP4 – 2/2**

EMPRESA A AUDITAR	HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE

VALORES CORPORATIVOS

9. **Pertenencia**: Nuestros funcionarios inician sus labores con sentido de pertenencia que permita mantener la cohesión humana. Con amor por su trabajo, que además de ser una bendición, es un privilegio hacer parte de esta entidad, participando en las actividades que permitan generar una relación intragrupal, fortaleciendo el sentimiento de que todos somos uno.

10. **Lealtad:** Los funcionarios son fieles a las políticas, acuerdos y principios éticos por el cual se rige la entidad, buscando el cumplimiento de sus objetivos, con plena conciencia de servicio a la comunidad.

11. **Creatividad:** Nuestro entorno de trabajo es emocionalmente positivo. Innovamos permanentemente del tal forma que cada una de las áreas funcionales están motivadas a propiciar cambios en el diseño de nuestros servicios.

12. **Objetividad:** Los funcionarios ven los problema s del entorno con un enfoque que equilibre adecuadamente nuestra realidad, permitiendo ser justos ante los acontecimientos internos y externos, para obrar coherentemente tomando decisiones más eficientes que generen impacto en la región.

13. **Servicio:** Somos conscientes que nuestra principal responsabilidad es brindar atención en salud con calidad y calidez, satisfaciendo las necesidades y expectativas del paciente, familia y comunidad.

DOCUMENTO PREPARADO POR:	GERARDO CESAR MOSQUERA QUINTERO JORGE ARMANDO SARAVIA ALVERNIA JOSÉ JULIÁN PACHECO PÉREZ

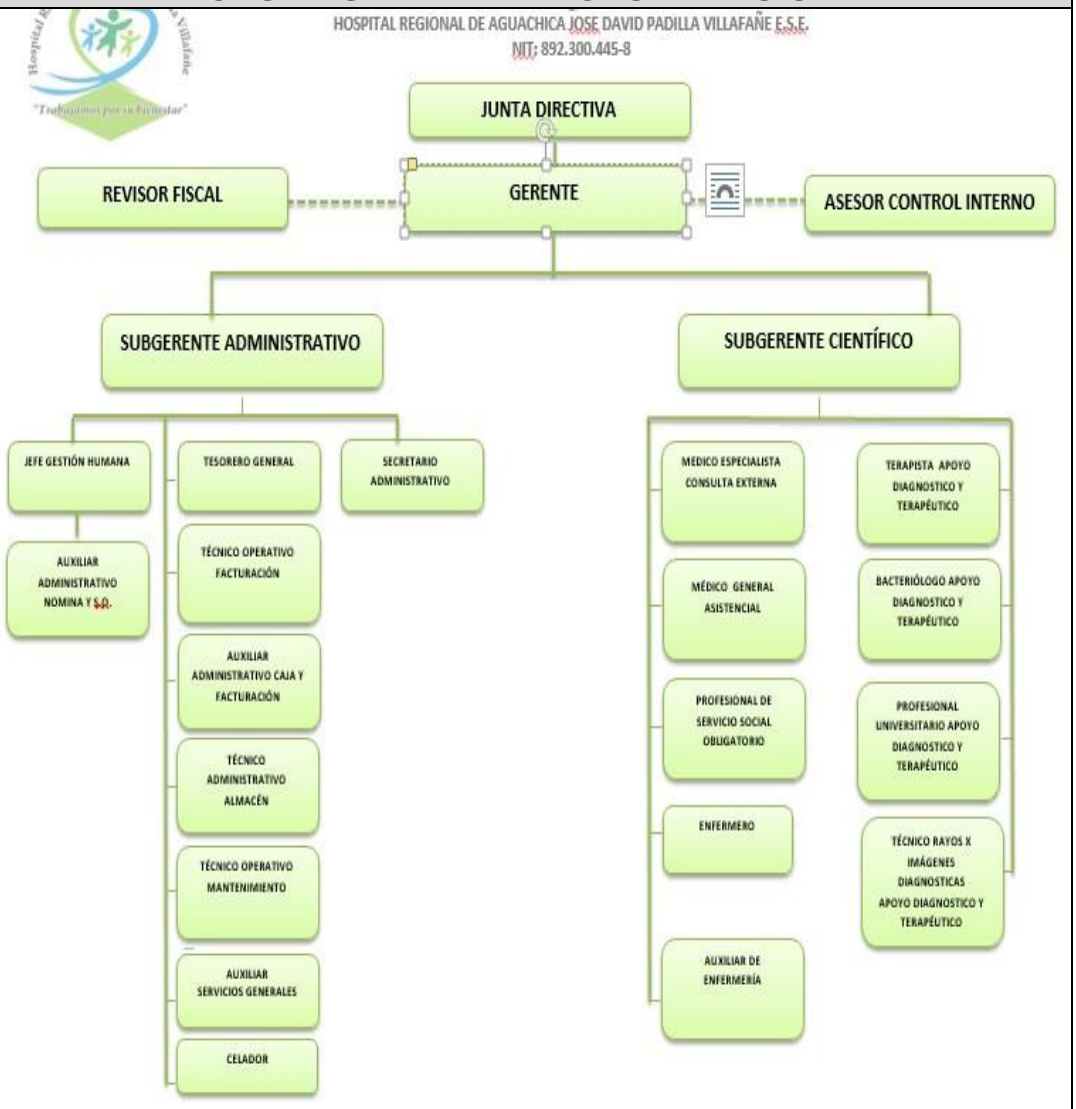
FUENTE: **HOSPITAL**

2.1.5 Organigrama de la organización

CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas	**AP5 – 1/1**

EMPRESA A AUDITAR HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE

ORGANIGRAMA DE LA ORGANIZACIÓN



DOCUMENTO PREPARADO POR:	GERARDO CESAR MOSQUERA QUINTERO JORGE ARMANDO SARAVIA ALVERNIA JOSÉ JULIÁN PACHECO PÉREZ

FUENTE: HOSPITAL

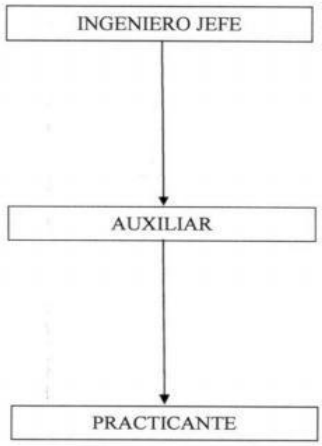
2.1.6 Organigrama del área de sistemas

CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas	**AP6 – 1/1**
EMPRESA A AUDITAR	**HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE**

ORGANIGRAMA DEL ÁREA DE SISTEMAS

REPUBLICA DE COLOMBIA
SECRETARIA DE SALUD DEPARTAMENTAL DEL CESAR
HOSPITAL REGIONAL DE AGUACHICA
JOSE DAVID PADILLA VILLAFAÑE
E.S.E.
NIT: 892.300.445-8

9. ESTRUCTURA OFICINA DE SISTEMAS



DOCUMENTO PREPARADO POR:	GERARDO CESAR MOSQUERA QUINTERO JORGE ARMANDO SARAVIA ALVERNIA JOSÉ JULIÁN PACHECO PÉREZ

FUENTE: HOSPITAL

2.1.7 Normas y políticas de seguridad de la información

CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas			**AP7 – 1/1**
EMPRESA A AUDITAR	HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE		
UNIDAD ADMINISTRATIVA DEPENDENCIA	SUBGERENCIA ADMINISTRATIVA SISTEMAS		
NORMAS Y POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN			
No.	**DESCRIPCIÓN**	**REFERENCIA**	**ULTIMA ACTUALIZACIÓN**
1	PLAN DE CONTINGENCIAS	SIS-POL-SG-001	2014
2	POLÍTICAS DE RECUPERACIÓN DE DATOS	SIS-POL-SG-002	2014
4	POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	SIS-POL-SG-004	2014
1	MAPA DE RIESGOS	SIS-DOC-SG-001	2014
DOCUMENTO PREPARADO POR:		GERARDO CESAR MOSQUERA QUINTERO JORGE ARMANDO SARAVIA ALVERNIA JOSÉ JULIÁN PACHECO PÉREZ	

FUENTE: HOSPITAL

2.1.8 Inventario de hardware

CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas		**AP8 – 1/1**
EMPRESA A AUDITAR	HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE	
UNIDAD ADMINISTRATIVA DEPENDENCIA	SUBGERENCIA ADMINISTRATIVA SISTEMAS	
INVENTARIO DE HARDWARE		
RESPONSABLE		**REFERENCIA DE EQUIPO**
RELACIONADOS EN EL MODULO DE ACTIVOS FIJOS DEL HOSPITAL		SISTEMAS DE INFORMACION

DOCUMENTO PREPARADO POR:	GERARDO CESAR MOSQUERA QUINTERO JORGE ARMANDO SARAVIA ALVERNIA JOSÉ JULIÁN PACHECO PÉREZ

FUENTE: EQUIPO AUDITOR

2.2 ARCHIVOS CORRIENTES

2.2.1 Programa general

CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas	**AC1 – 1/2**
EMPRESA A AUDITAR HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE **UNIDAD ADMINISTRATIVA** SUBGERENCIA ADMINISTRATIVA **DEPENDENCIA** SISTEMAS	
PROGRAMA DE AUDITORIA	
Denominación de la línea de auditoria	El trabajo de Auditoria se realizara en todas las áreas del Hospital Regional José Padilla Villafañe, en las cuales se procese o almacene información.
Objetivo general	Evaluar la seguridad física y ambiental en el Hospital Regional de Aguachica José David Padilla Villafañe ESE. basados en el estándar internacional ISO/IEC 27002:2013
Objetivo específicos	Evaluar la documentación de las políticas de seguridad física y ambiental empleadas en la organización. Revisar y evaluar los controles y lineamientos implementados en las políticas de seguridad física y ambiental por la organización. Revisar las actualizaciones, retroalimentaciones y divulgaciones realizadas respecto a las políticas de seguridad física y ambiental.
Fuente de criterios	ISO 27002 de 2013 Documentos: Archivos permanentes obtenidos de la organización.

<table>
<tr><td>Alcance de la auditoria</td><td colspan="2">La auditoría se realizará en todas las áreas del Hospital Regional José Padilla Villafañe, en las cuales se procese o almacene información, basándose en estándar internacional ISO/IEC 27002:2013</td></tr>
<tr><td>Justificación de la auditoria</td><td colspan="2">Servirá como soporte para la evaluación de las políticas existentes y sus controles y a su vez para la elaboración de un plan de mejoramiento.</td></tr>
<tr><td>Personal del área auditada</td><td colspan="2">Empleados de las diferentes áreas del Hospital.</td></tr>
<tr><td>Equipo auditor</td><td colspan="2">GERARDO CESAR MOSQUERA (GM)
JORGE ARMANDO SARAVIA (JS)
JOSÉ JULIÁN PACHECO PÉREZ(JP)</td></tr>
<tr><td rowspan="7">Presupuesto</td><td colspan="2">Recurso Materiales</td></tr>
<tr><td>Elementos de oficina</td><td>Lápiz, bolígrafos, hojas</td></tr>
<tr><td colspan="2">Recurso de Hardware</td></tr>
<tr><td>equipos</td><td>3. Portatiles
2. Usb</td></tr>
<tr><td colspan="2">Recurso de Software</td></tr>
<tr><td>Sistema operativo</td><td>Windows 7 Ultimate</td></tr>
<tr><td>Software de aplicación</td><td>Microsoft office</td></tr>
<tr><td rowspan="5">Presupuesto de horas estimada</td><td>Fase</td><td>Horas</td></tr>
<tr><td>Planificación</td><td>4</td></tr>
<tr><td>Programación</td><td>10</td></tr>
<tr><td>Ejecución de la Auditoria</td><td>120</td></tr>
<tr><td>Dictamen Resultados</td><td>6</td></tr>
<tr><td>DOCUMENTO PREPARADO POR:</td><td>Horas Estimadas</td><td>140</td></tr>
<tr><td colspan="3">GERARDO CESAR MOSQUERA QUINTERO
JORGE ARMANDO SARAVIA ALVERNIA
JOSÉ JULIÁN PACHECO PÉREZ</td></tr>
</table>

2.2.2 Situaciones encontradas

CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas			**AC2 – 1/2**
EMPRESA A AUDITAR HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE			
SITUACIONES ENCONTRADAS			
Situación	**Causas**	**Solución**	**Responsable**
Cuando el personal de turno de las áreas de enfermería abandona en su totalidad las estaciones, estas quedan desprotegidas y vulnerables a cualquier robo o alteración de información.	El área física de las estaciones de enfermería no puede ser cerrada en su totalidad por motivos de rapidez en las atenciones de urgencias.	Ubicar cámaras de seguridad que monitoreen las estaciones de enfermería, además de la ronda periódica del servicio de vigilancia.	Administración
Se evidencia falta de control por el servicio de vigilancia hacia el personal que entra a las diferentes áreas del Hospital.	Los empleados no portan permanentemente el carnet que los identifique como funcionarios del Hospital y los terceros tampoco llevan identificación visible	Carnetizar a todo los funcionarios que presten servicios para el Hospital a la vez que se le deberá exigir su portabilidad dentro de la institución. De igual manera identificar con algún mecanismo (ejm. carnet) a todo el personal que entra al Hospital.	Administración.
La gran mayoría de los empleados y terceros relacionados con el hospital, desconocen las políticas de seguridad del hospital	No se divulgaron las políticas de seguridad de la institución.	Socializar con el personal de la institución y terceros las políticas de seguridad del hospital.	Administración – Control Interno. Sistemas – gestión humana
No se hayo evidencia alguna de la divulgación de las políticas de	No se divulgaron las políticas de seguridad de la institución.	Socializar con el personal de la institución y terceros las políticas de	Administración – Control Interno.

seguridad del hospital.		seguridad del hospital.	Sistemas
Si bien el Hospital cuenta con las protecciones necesarias para evitar daños por fuego, no se cuenta con (alarmas, detectores) que contribuyan para una rápida reacción advirtiendo la presencia de factores externos causantes de desastres.	Faltan de sensores automáticos como alarmas y detectores que adviertan la presencia de peligro.	Instalación de sensores y alarmas	Administración
Se evidencia por la encuesta aplicada que el 20% de los empleados desconocen la ubicación de los extintores y el 63% nunca ha recibido capacitación para el manejo de los mismos.	Falta de capacitación al personal sobre la ubicación y el correcto uso de extintores y la forma de actuar frente al peligro por fuego.	Capacitar al personal de la institución sobre la ubicación y el correcto uso de extintores y la forma de actuar frente al peligro por fuego.	Administración
Se evidenciaron botellas con bebidas y comidas en algunos escritorios de trabajo	No se evidencio de ninguna forma que a los funcionarios del hospital se les prohibiera comer, beber o fumar cerca de los equipos de cómputo o lugares donde se procesa o almacena información.	Informar a los funcionarios sobre dichas prohibiciones y generar responsabilidad en ellos para el cumplimiento de las mismas.	Administración
La institución esta desprotegida contra problemas ocasionados por tormentas eléctricas.	No se cuenta con un para rayos	Realizar un estudio que determine la necesidad de instalar un para rayos de protección y de ser necesario, instalarlo	Administración – Sistemas
Los responsables de los equipos de cómputo desconocen el día que les fue asignado el mantenimiento	Falta de divulgación del plan de	Divulgar del plan de mantenimiento	Sistemas

preventivo de los equipos a su cargo motivo por el cual no programan sus tareas cotidianas con el fin de desocupar dicho equipo para la realización del mantenimiento, quedando este en ocasiones sin la realización del mismo.	mantenimiento con los empleados y áreas responsables de los equipos de cómputo.	con los empleados y áreas responsables de los equipos de cómputo.	
Se desconoce el porcentaje de ejecución real del plan de mantenimiento de equipos de cómputo.	Las planillas en las que se registra el mantenimiento realizado no son diligenciadas en su totalidad y cada vez que se realiza el mantenimiento.	Diligenciar las planillas siempre que se realice un mantenimiento y en su totalidad.	Sistemas
Se observó que aunque solo el 35% de los empleados encuestados dicen conocer políticas que reglamenten la salida de equipos de cómputo de las dependencias del Hospital, no se encuentra documento alguno que reglamente dicha política ni documento que responsabilice el empleado.	Falta de inclusión en las políticas de seguridad de la institución y divulgación de las mismas con los empleados y áreas responsables de los equipos de cómputo.	Actualizar las políticas de seguridad, incluyendo las necesarias para reglamentar la salida de equipos de cómputo de las dependencias del Hospital Falta de inclusión en las políticas de seguridad de la institución y divulgación de las mismas con los empleados y áreas responsables de los equipos de cómputo.	Administración – Control Interno. Sistemas – Gestión Humana.
Se observó que aunque solo el 35% de los empleados encuestados dicen conocer políticas que reglamenten la salida de equipos de cómputo del Hospital, no se encuentra documento alguno que reglamente dicha política.	Falta de inclusión en las políticas de seguridad de la institución y divulgación de las mismas con los	Actualizar las políticas de seguridad, incluyendo las necesarias para reglamentar la salida de equipos de cómputo del Hospital Falta de	Administración – Control Interno. Sistemas

	empleados y áreas responsables de los equipos de cómputo.	inclusión en las políticas de seguridad de la institución y divulgación de las mismas con los empleados y áreas responsables de los equipos de cómputo.	
Aunque en las áreas administrativas y centro de cómputo no se permite la presencia de terceros sin previa autorización y supervisión, el 14% de los encuestados correspondientes al área asistencial manifestó lo contrario debido a que por la ubicación de su área la presencia de pacientes es muy alta y en momentos de emergencia donde el personal de atención se desplace de su área, quedan los equipos desatendidos y vulnerables. Por otro lado se observó en inspección de campo que la gran mayoría de usuarios dejan la sesión del sistema de información abierta mientras se ausentan de su lugar de trabajo.	Falta de controles para evitar la presencia de usuarios no autorizados en áreas de almacenamiento o procesamiento de información y la no concientización de los usuarios para cerrar su sesión de trabajo cada vez que se retiren del computador.	Implementar controles para evitar la presencia de usuarios no autorizados en áreas de almacenamiento o procesamiento de información y concientizar a los usuarios para cerrar su sesión de trabajo cada vez que se retiren del computador.	Administración – Usuarios
No se halló evidencias de la socialización con los empleados, revisión y actualización de las políticas de seguridad.	Descuido por parte de la gerencia y el encargado de la dependencia de sistemas	Realizar el lanzamiento y puesta en marcha de las diferentes políticas de seguridad cumpliendo los lineamientos exigidos por la ISO 27002:2013.	Control interno – Sistemas

2.2.3 Instrumentos de recolección de datos

2.2.3.1 Encuesta

Co la siguiente encuesta, se pretende obtener información que contribuya al establecimiento del estado actual del hospital, con respecto a la seguridad física y ambiental.

ENCUESTA DIRIGIDA A LOS EMPLEADOS DEL HOSPITAL REGIONAL JOSE PADILLA VILLAFAÑE

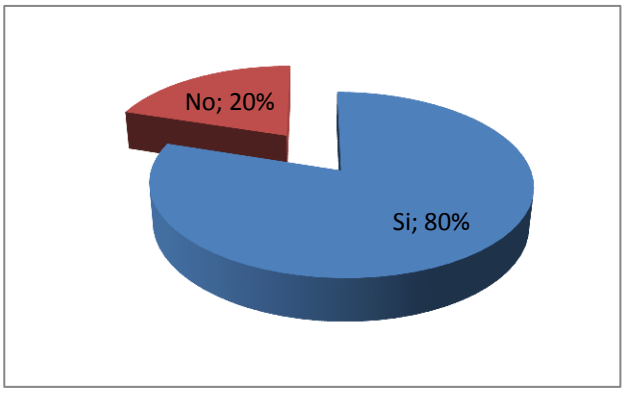
Control 11.1.1 Perímetro De Seguridad Física.

Tabla 1. ¿Su área de trabajo le brinda seguridad contra el acceso no autorizado a terceros?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	110	80%
No	27	20%
Total	137	100%

Fuente: Autores del proyecto

Figura 1. Seguridad contra el acceso no autorizado a terceros



Fuente: Autores del proyecto

Interpretación: La grafica anterior nos muestra que la mayoría del personal encuestado manifiesta sentir que su área de trabajo si le brinda seguridad contra el acceso no autorizado. Aquellos que manifestaron sentirse inseguros son en gran parte empleados de las áreas asistenciales, las cuales por motivo de agilidad en el servicio no pueden tener un perímetro cerrado.

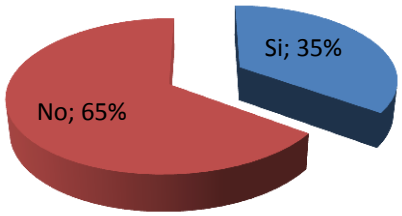
Control 11.1.2 Controles Físicos De Entrada.

Tabla 2. ¿Porta permanentemente un carnet que lo identifique como empleado del hospital?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	48	35%
No	89	65%
Total	137	100%

Fuente: Autores del proyecto

Figura 2. Utilización de carnet



Fuente: Autores del proyecto

Interpretación: La grafica anterior nos muestra que la mayor parte de los empleados no portan permanentemente el carnet que los identifique como empleados del hospital, impidiendo de esta manera que el personal de seguridad del hospital puedan controlar el acceso a las distintas áreas del mismo por personal externo ya que no se pueden identificar a los empleados del resto de usuarios del hospital.

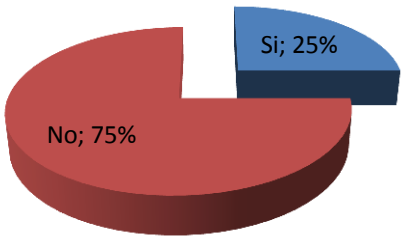
Control 11.1.3 Seguridad De Oficinas, Despachos Y Recursos.

Tabla 3. ¿Conoce las políticas de seguridad de la información del hospital?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	34	25%
No	103	75%
Total	137	100%

Fuente: Autores del proyecto

Figura 3. Conocimientos de las políticas de la seguridad de la información



Fuente: Autores del proyecto

Interpretación: La grafica anterior nos muestra que la mayoría de los empleados desconocen las políticas de seguridad de la información del hospital. Esto con lleva a que el personal desconociendo las normas y procedimientos establecidos por el hospital pueda poner en riesgo la información y los activos de la institución.

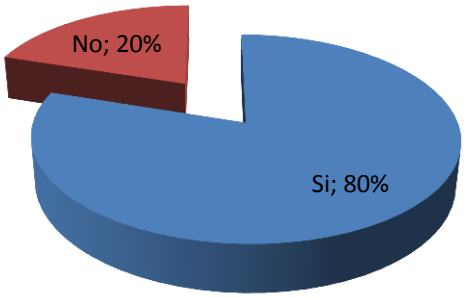
Control 11.1.4 Protección Contra Las Amenazas Externas Y Ambientales.

Tabla 4. ¿Conoce la ubicación de los extintores en su área de trabajo?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	110	80%
No	27	20%
Total	137	100%

Fuente: Autores del proyecto

Figura 4. Conocimiento ubicación de Extintores en el Área de trabajo



Fuente: Autores del proyecto

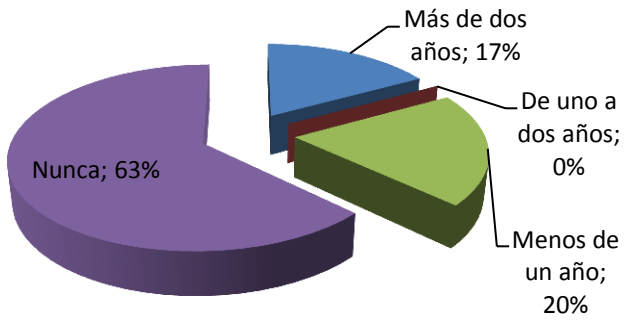
Interpretación: Es de reconocer que si bien un gran porcentaje de los empleados conoce la ubicación de los extintores, no deja de ser preocupante que haya un 20 % de los empleados que desconocen su ubicación, poniendo en riesgo el área, sus activos, información y empleados en caso de incendios.

Tabla 5. ¿Cuándo fue la última vez que recibió una capacitación en el uso de equipos contraincendios?

RESPUESTA	CANTIDAD	PORCENTAJE
Más de dos años	23	17%
De uno a dos años	0	0%
Menos de un año	27	20%
Nunca	87	63%
Total	137	100%

Fuente: Autores del proyecto

Figura 5. Capacitación de equipos contraincendios



Fuente: Autores del proyecto

Interpretación: La grafica anterior nos muestra que el 63% de los empleados manifiestan que nunca han recibido capacitación en el uso de equipos contraincendios, evidenciando una gran vulnerabilidad puesto que por el desconocimiento de su uso no se podría actuar eficientemente contra una emergencia causada por fuego, poniendo en riesgo el área, sus activos, información y empleados en caso de incendios.

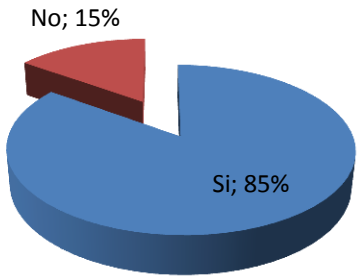
Control 11.2.1 Emplazamiento Y Protección De Equipos

Tabla 6. ¿Se le ha dado a conocer alguna directriz que le impida comer, fumar o beber cerca de los equipos de cómputo?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	116	85%
No	21	15%
Total	137	100%

Fuente: Autores del proyecto

Figura 6. Conocimiento directriz que le impidan comer fumar o beber cerca de los equipos.



Fuente: Autores del proyecto

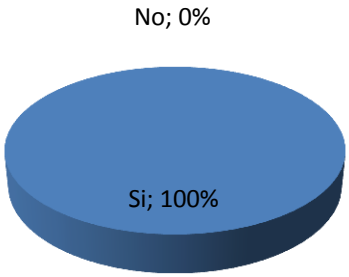
Interpretación: La grafica muestra que la mayor parte de los empleados afirman conocer las directrices que le impiden comer, fumar y beber cerca de los equipos de cómputo manteniendo un comportamiento y sentido de pertenencia hacia los activos del hospital, más aún deben tomarse medidas que aseguren que la totalidad de los empleados conozcan y cumplan con estas normas para evitar posibles accidentes con equipos electrónicos.

Tabla 7. ¿Conoce el inventario de equipos informáticos a su cargo?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	137	100%
No	0	0%
Total	137	100%

Fuente: Autores del proyecto

Figura 7. Inventario equipos a su cargo



Fuente: Autores del proyecto

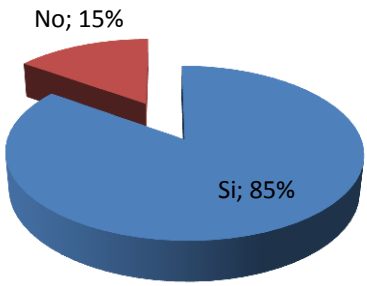
Interpretación: La grafica muestra que todos los empleados conocen el inventario de equipos informáticos a su cargo. En caso de pérdidas, alteración o daños de activos no podrán evadir responsabilidades y servirá de primer control para la protección por perdida.

Tabla 8. ¿Considera que su área de trabajo y su ambiente laboral permiten una eficaz protección a los equipos informáticos?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	116	85%
No	21	15%
Total	137	100%

Fuente: Autores del proyecto

Figura 8. Conocimiento a la protección de los equipos informáticos



Fuente: Autores del proyecto

Interpretación: La grafica muestra que la mayoría del personal encuestado considera que su área y su ambiente laboral si permiten una eficaz protección a los equipos informáticos. Aquellos que manifestaron sentirse inseguros son en gran parte empleados de las áreas asistenciales, las cuales por motivo de agilidad en el servicio no pueden tener un perímetro cerrado y dependen de terceros para su protección.

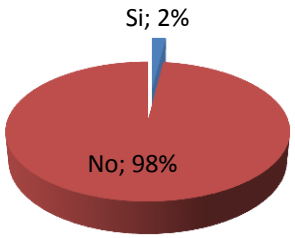
Control 11.2.2 Instalaciones de suministro

Tabla 9. ¿Su trabajo se ha visto interrumpido por falla en el fluido eléctrico o en las telecomunicaciones?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	3	2%
No	134	98%
Total	137	100%

Fuente: Autores del proyecto

Figura 9. Trabajo suspendido por fallas eléctricas o en telecomunicaciones



Fuente: Autores del proyecto

Interpretación: La grafica indica que la mayoría de los trabajadores indican que la labor no ha sido interrumpida por fallas eléctricas y de telecomunicaciones demostrando que el hospital ha contado con los mecanismos de protección eléctrica y varios operadores de telecomunicaciones que permitan la continuidad laboral del hospital ofreciendo el mejor servicio a la comunidad.

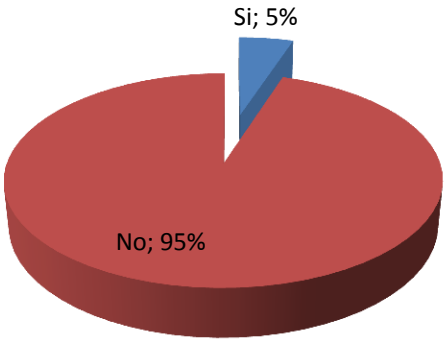
Control 11.2.4 Mantenimiento De Los Equipos.

Tabla 10. ¿Se le dio a conocer con anterioridad las fechas en las que se realizaría mantenimiento preventivo a los equipos de cómputo a su cargo?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	7	5%
No	130	95%
Total	137	100%

Fuente: Autores del proyecto

Figura 10. Conocimientos de las fechas de los mantenimientos preventivos de los equipos de cómputo.



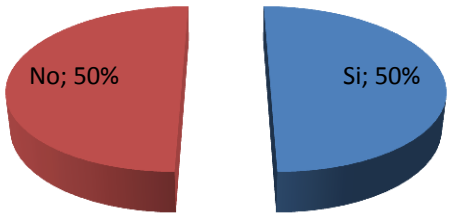
Fuente: Autores del proyecto

Interpretación: La grafica muestra que la mayor parte de la población no tiene conocimiento de las fechas en las que se realizará los mantenimientos preventivos de los equipos de cómputo. Por lo cual el trabajo de los empleados se ve interrumpido cada vez que se realicen ya que no existe un previo aviso o podrá no realizarse el mantenimiento debido a la importancia de la tarea realizada por el usuario acortando la vida útil de los mismos y poniendo en riesgo la información que en ellos se almacene.

Tabla 11. ¿Está satisfecho con los mantenimientos realizados a los equipos de cómputo a su cargo?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	68	50%
No	69	50%
Total		

Figura 11. Conformidad con los mantenimientos realizados



Fuente: Autores del proyecto

Interpretación: La grafica muestra que la mitad de la población no está conforme con los mantenimientos realizados a los equipos de cómputo a su cargo lo que evidencia que deben tomarse medidas que garanticen la satisfacción del servicio prestado y evitar posibles vulnerabilidades.

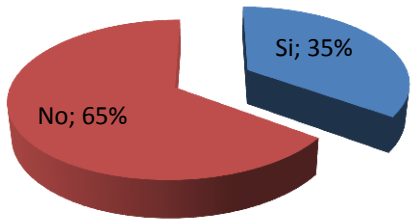
Control 11.2.5 Salida de activos fuera de las dependencias de la empresa

Tabla 12. ¿Conoce las políticas internas que regulan la salida de equipos de las dependencias del Hospital?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	48	35%
No	89	65%
Total	137	100%

Fuente: Autores del proyecto

Figura 12. Conocimiento de políticas para la salida de equipos fuera de las dependencias



Fuente: Autores del proyecto

Interpretación: La grafica muestra que la mayoría de los encuestados no conocen las políticas internas que regulan la salida de equipos de las dependencias del Hospital, esto podría ocasionar perdidas de activos e información por desconocimiento de dichos protocolos.

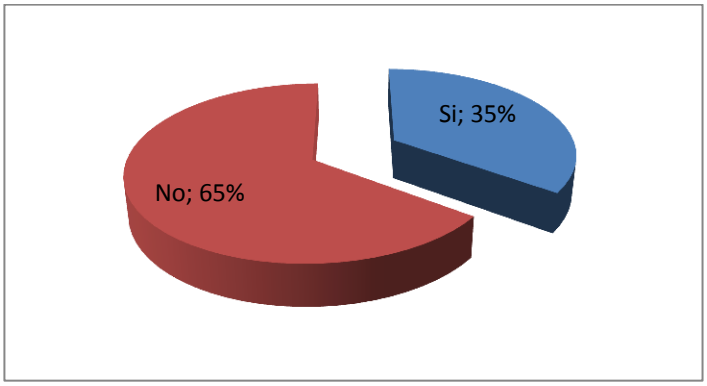
Control 11.2.6 Seguridad De Los Equipos Y Activos Fuera De Las Instalaciones.

Tabla 13. ¿Conoce las políticas internas que regulan la salida de equipos de cómputo del Hospital?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	48	35%
No	89	65%
Total	137	100%

Fuente: Autores del proyecto

Figura 13. Conocimientos de políticas para la salida de equipos fuera de las instalaciones.



Fuente: Autores del proyecto

Interpretación: La grafica indica que la mayoría de los encuestados desconocen las políticas internas que regulan la salida de equipos del Hospital por lo que puede ocasionar traslado de información confidencial y perdida de activos.

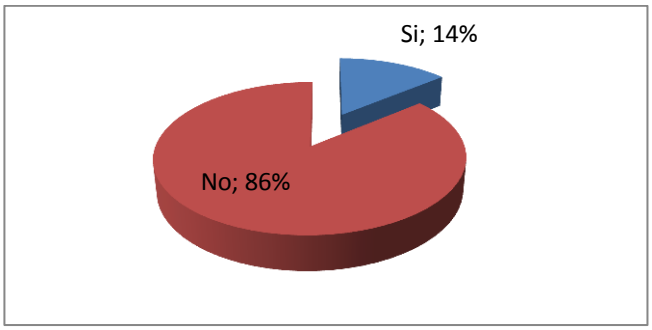
Control 11.2.8 Equipo Informático De Usuario Desatendido.

Tabla 14. ¿Al ausentarse de su área de trabajo queda personal no autorizado en ella?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	19	14%
No	118	86%
Total	137	100%

Fuente: Autores del proyecto

Figura 14. Personal no autorizado en su área



Fuente: Autores del proyecto

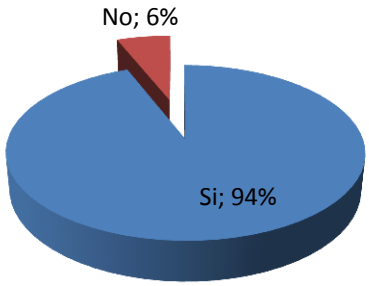
Interpretación: La grafica muestra que la mayoría de los encuestados al momento de ausentarse de su área de trabajo no queda en ella personal no autorizada. Garantizando que la información y los activos sean accedidos por terceros, sin embargo el 14% de los mismos indica lo contrario, evidenciando una vulnerabilidad en la protección de la información.

Tabla 15. ¿Cuándo sabe que su equipo va a quedar sin uso por tiempo prolongado lo apaga?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	129	94%
No	8	6%
Total	137	100%

Fuente: Autores del proyecto

Figura 15. Conocimiento de apagar equipo que no están en uso.



Fuente: Autores del proyecto

Interpretación: La grafica muestra que la gran parte de los encuestados al momento de ausentarse de su área de trabajo apagan los equipos. Debería por parte del hospital concientizar a todos los empleados sobre el apagado de los equipos desatendidos por largo tiempo con el fin de prolongar su vida útil.

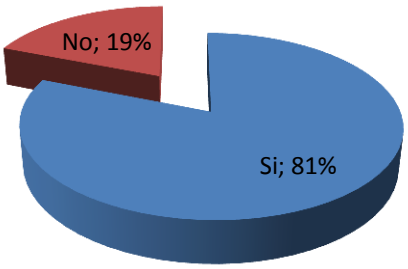
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

Tabla 16. ¿Cierra su sesión de trabajo en su computador cuando tiene que ausentarse de su puesto?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	111	81%
No	26	19%
Total	137	100%

Fuente: Autores del proyecto

Figura 16. Conocimiento de las políticas de trabajo despejado y bloqueo de pantalla



Fuente: Autores del proyecto

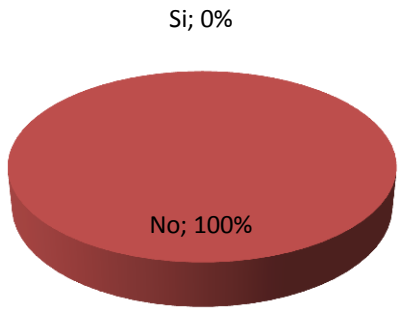
Interpretación: la gráfica indica que la mayoría de los encuestados cierran su sesión cuando se van ausentarse de su puesto evitando que terceros accedan sin autorización a los equipos informáticos más el 19 % no lo hacen, permitiendo así que cualquier persona pueda alterar o extraer la información por medio de su computador.

Tabla 17. ¿Sobre su escritorio queda información sensible cuando usted no se encuentra en su área de trabajo?

RESPUESTA	CANTIDAD	PORCENTAJE
Si	0	0%
No	137	100%
Total	137	100%

Fuente: Autores del proyecto

Figura 17. Deja Información sensible en su escritorio



Fuente: Autores del proyecto

Interpretación: la gráfica anterior muestra que todos los encuestados manifiestan no dejar información sensible cuando no se encuentra en su área de trabajo granizando la confidencialidad y seguridad de la información.

2.2.3.2 Listas de chequeo

LISTA DE CHEQUEO DIRIGIDA A LOS EMPLEADOS DE LA DIVISION DE SISTEMAS DEL HOSPITAL REGIONAL JOSE PADILLA VILLAFAÑE

INSTRUCCIONES: A continuación usted encontrara una serie de preguntas de las cuales debe responder con SI / NO.

NOMBRE DE LA EMPRESA	**HOSPITAL REGIONAL JOSE DAVID PADILLA VILLAFAÑE**
AREA AUDITADA	**SISTEMAS**
FORMATO DE VERIFICACION	
Dominio	11. SEGURIDAD FISICA Y AMBIENTAL
Objetivo de Control	11.1 AREAS SEGURAS – 11.2 SEGURIDAD DE LOS EQUIPOS
CUESTIONARIO	

Pregunta	Si	No	NA	Observaciones
11.1.1 Perímetro De Seguridad Física				
¿Se cuenta con perímetros de seguridad debidamente establecidos para la protección de equipos de cómputo que procesan información sensible para el Hospital?	**X**			
¿Hay establecida un área de recepción con personal u otros medios para controlar el acceso físico al centro de cómputo únicamente al personal autorizado?	**X**			
11.1.2 Controles Físicos De Entrada				
¿El centro de cómputo está protegido con controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado?	X			
¿El acceso a visitantes al centro de cómputo debe ser previamente autorizado?	X			
¿Se registra la fecha y la hora de entrada y salida de visitantes al centro de cómputo?	X			
¿Se supervisa el trabajo de los visitantes autorizados al centro de cómputo?	X			
¿Se exige identificación a los visitantes que manifiestan la intención de acceso autorizado al centro de cómputo?	X			
11.1.3 Seguridad De Oficinas, Despachos Y Recursos				
¿Cuenta el centro de cómputo con políticas de seguridad de la información documentada y aprobadas. ?	X			
¿Existen evidencias de la divulgación de políticas de seguridad?		X		No se evidencia documento que constate la divulgación de las políticas con los empleados.
11.1.4 Protección Contra Las Amenazas Externas Y Ambientales				
¿Existen protecciones físicas contra daño por incendio?	X			
¿Existen sensores automáticos que adviertan la presencia de condiciones anormales en el ambiente?		X		No se evidencio en el centro de cómputo la instalación de sensores o alarmas que cumplan dicho propósito.
¿Existen protecciones físicas contra			X	El área de ubicación del

daño por inundación, terremoto, y otras formas de desastre natural?				hospital posee bajo riesgo de ocurrencia de estos fenómenos.
¿Los equipos de repuesto y los medios de soporte de seguridad están ubicados a una distancia prudente para evitar daño debido a algún desastre que afecte a las instalaciones principales?	X			
¿Existe un equipo apropiado contra incendios y ubicado adecuadamente?	X			
11.1.5 El Trabajo En Áreas Seguras				
¿Se supervisa el trabajo no autorizado en áreas seguras tanto por razones de seguridad como para evitar las oportunidades de actividades maliciosas?	X			
¿Las áreas seguras vacías tienen un bloqueo físico y se revisan periódicamente?	X			
¿Los equipos de grabación fotográfica, de video, de audio y otros equipos de grabación como cámaras en dispositivos móviles, son restringidos y solo se ingresan con autorización?	X			
11.2.1 Emplazamiento Y Protección De Equipos				
¿Tiene el centro de cómputo protección contra rayos?		X		No se evidencio la instalación de para-rayos
¿Están separados los circuitos eléctricos de iluminación de los circuitos que alimentan los equipos?	X			
¿Está el centro de cómputo protegido de la luz solar directa?	X			
¿Es el techo del centro de cómputo impermeable para evitar el paso de agua desde niveles superiores?		X		Se evidencia la falta de impermeabilización del techo en el centro de cómputo.
¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del el centro de cómputo para evitar daños al equipo?		X		No se evidencio documento que constate la divulgación de dicha política.
¿Está instalada una alarma para detectar fuego (calor o humo) en forma automática?		X		No se evidencio la instalación de alarmas.
¿Se cuenta con medidores de humedad relativa en el centro de cómputo?		X		
11.2.2 Instalaciones De Suministro				
¿Los equipos están protegidos contra	X			

fallas en el suministro de energía y otras anomalías causadas por fallas en los servicios de suministro?				
¿Existe dos o más proveedores del servicio para evitar que la falla en una ruta de conexión elimine los servicios de voz?	X			
¿Se cuentan con equipos refrigerantes (aires acondicionados) en el centro de cómputo?				
11.2.3 Seguridad Del Cableado				
¿Existe protección adecuada contra interceptaciones o daños para el cableado de energía eléctrica y de telecomunicaciones que transporta datos o presta soporte a los servicios de información?	X			
¿Está el cableado de la red protegido contra interceptación no autorizada o daño, utilizando conductos o evitando rutas a través de áreas públicas?	X			
¿Están los cables de energía debidamente separados de los cables de comunicaciones para evitar interferencia?	X			
¿Se cuenta con un plano del cableado estructurado para reducir la posibilidad de errores?	X			
¿Realizan reconocimientos técnicos e inspecciones físicas en busca de dispositivos no autorizados conectados al cableado?	X			
11.2.4 Mantenimiento De Los Equipos				
¿Existe plan de mantenimiento de equipos para asegurar su continua disponibilidad e integridad?	X			
¿Existe planillas de mantenimiento debidamente diligenciadas de equipos de cómputo?		X		Al revisar las planillas de los mantenimientos ejecutados, se evidencio que el número de estas es inferior al número de mantenimientos que estaban programados para la fecha.
11.2.5 Salida De Activos Fuera De Las Dependencias De La Empresa				
¿Se lleva un registro de los equipos que salen de la dependencia hacia otra área?		X		No se evidencio el registro.
¿Existen políticas que reglamenten la salida de equipos informáticos hacia otras		X		No se evidencio políticas al respecto.

dependencias?				
11.2.6 Seguridad De Los Equipos Y Activos Fuera De Las Instalaciones				
¿Existe un control de seguridad hacia los equipos fuera de las instalaciones teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización?		X		No se evidencio el control.
¿Existen políticas que reglamenten la protección de los equipos fuera de las Instalaciones?		X		No se evidencio políticas al respecto.
11.2.7 Reutilización O Retirada Segura De Dispositivos De Almacenamiento				
¿Se verifican los elementos del equipo que contengan medios de almacenamiento para asegurar que se haya eliminado cualquier software licenciado y datos sensibles o asegurar que se hayan sobrescrito de forma segura, antes de la eliminación?	X			
¿Existe un control para los dispositivos deteriorados que determinen si los elementos se deberían destruir físicamente en lugar de enviarlos a reparación o desecharlos?	X			
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla				
¿Existen políticas que den directrices sobre el puesto de trabajo despejado y el bloqueo de pantalla?	X			
¿Al ausentarse los empleados de su puesto de trabajo, dejan documentos con expuestos información sensible o para la empresa.		X		Se evidencio la correcta aplicación de dicha política.

Lista de chequeo
Hospital José David Padilla Villafañe
Especialización en Auditoría de Sistemas

LISTA DE CHEQUEO DIRIGIDA A LOS EMPLEADOS DE LAS AREAS ADMINISTRATIVA Y ASISTENCIAL DEL HOSPITAL REGIONAL JOSE PADILLA VILLAFAÑE

INSTRUCCIONES: A continuación usted encontrara una serie de preguntas de las cuales debe responder con SI / NO.

NOMBRE DE LA EMPRESA	**HOSPITAL JOSE DAVID PADILLA VILLAFAÑE**			
AREA AUDITADA	**ADMINISTRACION – ASISTENCIAL**			
FORMATO DE VERIFICACION				
Dominio	11. SEGURIDAD FISICA Y AMBIENTAL			
Objetivo de Control	11.1 AREAS SEGURAS – 11.2 SEGURIDAD DE LOS EQUIPOS			
Cuestionario				
Pregunta	**Si**	**No**	**NA**	**Observaciones**
¿Se cuenta con perímetros de seguridad debidamente establecidos para la protección de equipos de cómputo que procesan información sensible para el Hospital?	**X**			Sin embargo se evidencia que en las estaciones de enfermería por razones de atención de urgencias no debe haber obstáculos que permitan la oportuna reacción del personal asistencial.
¿Las áreas están protegidas con controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado?	X			
¿El acceso a visitantes a las áreas debe ser previamente autorizado?	x			
¿Portan los empleados del hospital el carnet que los identifique como tales permanentemente?		X		Se evidencio que ningún empleado porto carnet de identificación institucional durante la auditoria realizada.
¿Existen protecciones físicas contra daño por incendio?	x			
¿Existen protecciones físicas contra daño por inundación, terremoto, y otras formas de desastre natural?			x	
¿Existe un equipo apropiado contra incendios y ubicado adecuadamente?	x			
¿Se lleva un registro de los equipos	X			

que salen de la dependencia hacia otra área?				
¿Se restringe el acceso al área de despacho y carga desde el exterior de la edificación a personal identificado y autorizado?	X			
¿El material que llega se inspecciona para determinar posibles amenazas antes de moverlo desde el área de despacho y carga hasta el punto de uso?	X			
¿El material que llega se registra de acuerdo con los procedimientos de gestión de activos a su entrada al lugar?	X			
¿Se cuentan con equipos refrigerantes (aires acondicionados) en el centro de cómputo?	X			

2.2.10 Pruebas de cumplimiento

CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistemas	**AC11 – 1/1**
NOMBRE DE LA EMPRESA: HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE	
UNIDAD ADMINISTRATIVA: DEPENDENCIA DE SISTEMAS	
PROCESO AUDITADO	EVALUACIÓN DE LAS POLÍTICAS DE SEGURIDAD
OBJETIVO	PROPORCIONAR EVIDENCIA DE LOS CONTROLES EXISTENTES Y QUE SEAN APLICADOS DE MANERA EFECTIVA EN LA DEPENDENCIA DE SISTEMAS.
PROCEDIMIENTOS	VERIFICAR EL CUMPLIMIENTO DE LAS POLÍTICAS EXISTENTES DE LA DEPENDENCIA DE SISTEMAS.
TÉCNICAS	INSPECCIÓN, OBSERVACIÓN DIRECTA, LISTAS DE CHEQUEO.
RECURSOS	FUENTES DE CRITERIO DE LA AUDITORIA
FECHA DE AUDITORIA	17/05/2014

HALLAZGO	NO SE ESTÁN CUMPLIENDO LAS POLÍTICAS EN CUANTO MANTENIEMIENTO DE EQUIPOS DE COMPUTO.
CAUSA	SE ENCONTRÓ QUE FALTA DE CONTROL EN LAS EVIDENCIAS DE LOS MANTENIMIENTOS REALIZADOS.
SITUACIÓN DE RIESGO	SI LOS MANTENIMIENTOS PREVENTIVOS NO SE REALIZAN OPORTUNAMENTE, LOS EQUIPOS ESTARÁN EXPUESTOS A MAL FUNCIONAMIENTO Y PROBABLE DAÑO.
RECOMENDACIÓN	DAR CUMPLIMIENTO ESTRICTO A LA POLITICA EN CUANTO A AL PLAN DE MANTENIMIENTO PROGRAMADO.
DOCUMENTO PREPARADO POR **GERARDO CESAR MOSQUERA QUINTERO** **JORGE ARMANDO SARAVIA ALVERNIA** **JOSÉ JULIÁN PACHECO PÉREZ**	
Fecha: 17 de Abril de 2014	**Fecha:** 17 de Mayo de 2014

1.2.2.11 Pruebas sustantivas

CSI AUDIS Consultores de Sistemas de Información - Auditores de Sistem	**AC12 – 1/1**
NOMBRE DE LA EMPRESA: HOSPITAL REGIONAL DE AGUACHICA JOSÉ DAVID PADILLA VILLAFAÑE	
UNIDAD ADMINISTRATIVA: DEPENDENCIA DE SISTEMAS	
PROCESO AUDITADO	EVALUACIÓN DE LAS POLÍTICAS DE SEGURIDAD
OBJETIVO	PROPORCIONAR EVIDENCIA DE LOS CONTROLES EXISTENTES Y QUE SEAN APLICADOS DE MANERA EFECTIVA EN LA DEPENDENCIA DE SISTEMAS
PROCEDIMIENTOS	VERIFICAR EL CUMPLIMIENTO DE LAS POLÍTICAS EXISTENTES DE LA DEPENDENCIA DE SISTEMAS.

TÉCNICAS	INSPECCIÓN, OBSERVACIÓN DIRECTA, LISTAS DE CHEQUEO.
RECURSOS	FUENTES DE CRITERIO DE LA AUDITORIA
FECHA DE AUDITORIA	17/05/2014
HALLAZGO	EL CENTRO DE COMPUTO ESTA ESPUESTO A FILTRACIONES DE AGUA.
CAUSA	EL TECHO NO SE ENCUENTRA IMPERMEABILIZADO
SITUACIÓN DE RIESGO	AL SER LA EDIFICACION TAN ANTIGUA, ES PROBABLE QUE DURANTE UNA TORMENTA, SE FILTRE AGUA POR EL TECHO Y AFECTE LOS EQUIPOS ELECTRONICOS
RECOMENDACIÓN	IMPERMEABILIZAR EL TECHO DEL CENTRO DE COMPUTO.
DOCUMENTO PREPARADO POR **GERARDO CESAR MOSQUERA QUINTERO** **JORGE ARMANDO SARAVIA ALVERNIA** **JOSÉ JULIÁN PACHECO PÉREZ**	
Fecha: 17 de Abril de 2014	**Fecha:** 17 de Mayo de 2014

1.2.2.13 INFORME

INFORME

Aguachica 17 de Mayo de 2014

DOCTOR
EDWING ARMANDO VEGA CAVIEDES
GERENTE
Hospital Regional De Aguachica José David Padilla Villafañe E. S.
D.

Cordial saludo,

Como parte del desarrollo de la práctica de la Especialización de Auditoría de Sistemas, se procedió a efectuar una auditoria en la dependencia de Sistemas, adscrita a la Subdirección Administrativa del Hospital Regional De Aguachica José David Padilla Villafañe

El objetivo del ejercicio consistió en evaluar el cumplimiento de las políticas de seguridad según el estándar ISO 27002 de 2013 en un periodo comprendido del 14 de abril de 2014 al 17 de mayo de 2014.
De los resultados obtenidos durante la evaluación me permito informarle a Usted, las siguientes observaciones:

HALLAZGO 1.

CONDICIÓN: El personal del hospital está laborando dentro de la institución sin portar el carnet institucional.

CAUSA: Debido al cambio de empresas contratistas, no se están generando a tiempo la carnetización de los empleados y falta de control de la administración del hospital frente a esta situación.

EFECTO: Problemas de seguridad por acceso no autorizado a áreas restringidas del hospital.

RECOMENDACIÓN: Realizar inmediatamente la carnetización a todo el personal que labore en la Institución.

HALLAZGO 2.

Se evidencio que no hay documento que soporte la divulgación de las políticas de seguridad del hospital.

CONDICIÓN: En el Hospital, no se encuentran evidencias de la divulgación de las políticas de seguridad de la información.

CAUSA: las políticas no fueron divulgadas de una manera en la que todo el personal pudiera tener conocimiento de ellas, tanto así que se evidencia en el no registro de las personas a las que llego la información.

EFECTO: La no divulgación de las políticas de seguridad podría llevar a cometer errores en procedimientos que comprometerían la seguridad de la información y a la vez no se podría establecer responsabilidades, puesto que se desconocían las normas, comprometiendo de esta manera la continuidad del negocio.

RECOMENDACIÓN: Realizar la divulgación a todo el personal que labora en el hospital y registrar la participación de la misma.

HALLAZGO 3.

CONDICIÓN: El centro de cómputo carece de sensores que contribuyan para una rápida reacción advirtiendo la presencia de factores externos causantes de desastres.

CAUSA: Falta de gestión administrativa

EFECTO: Perdida de activos y compromiso en la continuidad del negocio.

RECOMENDACIÓN: Instalar inmediatamente sensores que monitoreen las condiciones ambientales y alarmas que adviertan lo sucedido.

HALLAZGO 4.

CONDICIÓN: Si bien el hospital, cuenta con los extintores suficientes para mitigar una emergencia por fuego, se evidencia que no todos las personas que laboran en la institución conocen la ubicación y el correcto uso de los mismos.

CAUSA: falta de capacitación al personal sobre manejo de extintores y la ubicación de los mismos dentro del Hospital.

EFECTO: perdida de activos del Hospital y riesgo en la salud de las personas que se encuentran durante la emergencia por no saber la ubicación de los extintores y manejarlos adecuadamente.

RECOMENDACIÓN: capacitar al personal sobre manejo de extintores y divulgar la ubicación de los mismos dentro del Hospital.

HALLAZGO 5.

CONDICIÓN: Se hallaron botellas con bebidas en algunas áreas del hospital cerca de equipos de cómputo y no se evidencio documento que constate la divulgación de políticas, donde se prohíba comer, beber o fumar cerca de los mismos.

CAUSA: las políticas no fueron divulgadas de una manera en la que todo el personal pudiera tener conocimiento de ellas, tanto así que se evidencia en el no registro de las personas a las que llego la información.

EFECTO: El comer, beber o fumar cerca de los equipos de cómputo, podría causar accidentes que afecten a dichos equipos, comprometiendo así la información procesada y almacenada, así como la continuidad del negocio.

RECOMENDACIÓN: Realizar la divulgación a todo el personal que labora en el hospital y registrar la participación de la misma.

HALLAZGO 6.

CONDICIÓN: No se evidencio en el Hospital la implementación de un sistema de protección contra rayos

CAUSA: Al no ser una zona de alta frecuencia en tormentas eléctricas, se ha descuidado este mecanismo de seguridad.

EFECTO: Al caer un rayo o suficientemente cerca d las redes eléctricas del hospital, se podrían comprometer el correcto funcionamiento de estas y la perdida de equipos electrónicos por sobrecarga eléctrica, perdiendo asi la información y comprometiendo la continuidad del negocio.

RECOMENDACIÓN: Realizar un estudio que determine la necesidad de implementar un sistema de protección contra rayos y de ser viable implementarlo.

HALLAZGO 7.

CONDICIÓN: Si bien existe el documento "plan de mantenimiento preventivo", no se evidencia documento alguno que demuestre la divulgación del mismo.

CAUSA: Falta de gestión por el encargado del área de sistemas.

EFECTO: Si los responsables de los equipos de cómputo desconocen el día que les fue asignado el mantenimiento preventivo de los equipos a su cargo, podría ser este el motivo por el cual no programan sus tareas cotidianas con el fin de desocupar dicho equipo para la realización del mantenimiento, quedando este en ocasiones sin la realización del mismo y exponiéndose a daños que conllevarían a posible pérdida de información.

RECOMENDACIÓN: Divulgar del plan de mantenimiento con los empleados y áreas responsables de los equipos de cómputo y registrar la planilla que certifique la divulgación del plan.

.

HALLAZGO 8.

CONDICIÓN: Se evidencio que las planillas en las que se registra el mantenimiento realizado a los equipos de cómputo, no son diligenciadas en su totalidad y cada vez que se realiza el mantenimiento. Se desconoce el porcentaje de ejecución real del plan de mantenimiento de equipos de cómputo.

CAUSA: falta de gestión por el encargado del área mantenimiento

EFECTO: el desconocimiento de la ejecución del plan de mantenimiento podrá causar repetición en los mantenimientos programados y desatención en los equipos faltantes, ocasionando así un reproceso y retrasos innecesarios, a la vez que no permitirá llevar control sobre dicho plan.

RECOMENDACIÓN: Diligenciar las planillas siempre que se realice un mantenimiento y en su totalidad.

HALLAZGO 9.

CONDICIÓN: Se observó que aunque solo el 35% de los empleados encuestados dicen conocer políticas que reglamenten la salida de equipos de cómputo de las dependencias

ni del hospital, no se encuentra documento alguno que reglamente dicha política ni documento que responsabilice el empleado.

CAUSA: Falta de inclusión en las políticas de seguridad de la institución y divulgación de las mismas con los empleados y áreas responsables de los equipos de cómputo.

EFECTO: Al no incluir estas políticas, ni divulgarlas, así como resaltar la responsabilidad que estas implican al personal, podrían ser causantes de la desatención por parte del personal de los activos que tiene a su cargo permitiendo de esta manera daños, robos o alteraciones en los quipos a su cuidado.

RECOMENDACIÓN: Actualizar las políticas de seguridad, incluyendo las necesarias para reglamentar la salida de equipos de cómputo de las dependencias del Hospital, divulgarlas resaltando la responsabilidad que adquiere el personal de la Institución.

HALLAZGO 10.

CONDICIÓN: Si bien en las áreas administrativas y centro de cómputo no se permite la presencia de terceros sin previa autorización y supervisión, el 14% de los encuestados correspondientes al área asistencial manifestó lo contrario debido a que por la ubicación de su área la presencia de pacientes es muy alta y en momentos de emergencia donde el personal de atención se desplace de su área, quedan los equipos desatendidos y vulnerables con la sesión de usuario activa.

CAUSA: Una emergencia no da lugar para cerrar una sesión adecuadamente puesto que por estar en juego la vida de pacientes prima la rápida atención.

EFECTO: Al dejar el lugar de trabajo desatendido y la sesión de usuario activa, se da lugar a pérdidas de activos y manipulación indebida de la información, comprometiendo la integridad de los datos.

RECOMENDACIÓN: Implementar controles para evitar la presencia de usuarios no autorizados en áreas de almacenamiento o procesamiento de información y concientizar a los usuarios para cerrar su sesión de trabajo cada vez que se retiren del computador, así como programas los computadores para que se inactive la sesión a determinado tiempo de inactividad.

HALLAZGO 11.

CONDICIÓN: Si bien en las áreas administrativas y centro de cómputo no se permite la presencia de terceros sin previa autorización y supervisión, el 14% de los encuestados correspondientes al área asistencial manifestó lo contrario debido a que por la ubicación de su área la presencia de pacientes es muy alta y en momentos de emergencia donde el personal de atención se desplace de su área, quedan los equipos desatendidos y vulnerables con la sesión de usuario activa.

CAUSA: Una emergencia no da lugar para cerrar una sesión adecuadamente puesto que por estar en juego la vida de pacientes prima la rápida atención.

EFECTO: Al dejar el lugar de trabajo desatendido y la sesión de usuario activa, se da lugar a pérdidas de activos y manipulación indebida de la información, comprometiendo la integridad de los datos.

RECOMENDACIÓN: Implementar controles para evitar la presencia de usuarios no autorizados en áreas de almacenamiento o procesamiento de información y concientizar a los usuarios para cerrar su sesión de trabajo cada

EFECTO: Al dejar el lugar de trabajo desatendido y la sesión de usuario activa, se da lugar a pérdidas de activos y manipulación indebida de la información, comprometiendo la integridad de los datos.

RECOMENDACIÓN: Implementar controles para evitar la presencia de usuarios no autorizados en áreas de almacenamiento o procesamiento de información y concientizar a los usuarios para cerrar su sesión de trabajo cada vez que se retiren del computador, así como programas los computadores para que se inactive la sesión a determinado tiempo de inactividad.

Esperamos que la información proporcionada sea de utilidad para el mejoramiento continuo de la organización que usted dirige.

Gracias por la atención recibida.

JORGE ARMANDO SARAVIA ALVERNIA

LIDER AUDITOR