RESUMEN - TESIS DE GRADO

AUTORES	**HENRY MARULANDA PADILLA**
FACULTAD	**DE INGENIERÍAS**
PLAN DE ESTUDIOS	**INGENIERÍA DE SISTEMAS**
DIRECTOR	**Ing. MAGRETH ROSSIO SANGUINO REYES,**
TÍTULO DE LA TESIS	**EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER**

RESUMEN
(70 palabras aproximadamente)

El presente proyecto de pasantía surge a partir de la observación realizada en la Clínica San José S.A.S., cuyos activos en este caso la información, dispositivos de red, aplicaciones etc., se preservan en condiciones poco confiables, ya que no cuentan con las políticas, procedimientos, manuales, planes de contingencias formales para el resguardo de la información y la protección de la misma.

CARACTERÍSTICAS			
PÁGINAS: 224	PLANOS:	ILUSTRACIONES: 6	CD-ROM: 1

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER

HENRY MARULANDA PADILLA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2014

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

HENRY MARULANDA PADILLA

Informe final modalidad pasantías presentado para optar el título de Ingeniero de Sistemas

Director
Ing. MAGRETH ROSSIO SANGUINO REYES
Esp. Informática Educativa

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
INGENIERÍA DE SISTEMAS
OCAÑA
2014

AGRADECIMIENTOS

Como primera medida mi mayor agradecimiento a Dios que me dio fortaleza, paciencia y sabiduría para culminar con mucho éxito este proyecto tan fructífero.

A mi madre **Maribeth Padilla Cantillo**, que con su apoyo, amor, dulzura y santas oraciones me dieron fuerza para salir adelante y no dejarme vencer por todos los obstáculos presentados.

A mi papá **Henry Marulanda Rodríguez**, por su apoyo y su carácter fuerte que cada día me motivaba a salir adelante.

A mi hermana **Ludís Vanessa Blanco Padilla**, quien fue mi ejemplo a seguir en toda mi carrera profesional.

A mi hermano **Nelson Arturo Ramírez Padilla**, por creer en mí y darme fuerzas para salir adelante.

A mi novia **Maryuri Tatiana Ariza Prado**, quien fue pieza clave en todo este proceso, por su apoyo incondicional, su amor y ternura en todos esos momentos difíciles.

Y, finalmente, al resto de mi familia y amigos, por el apoyo que siempre he recibido.

CONTENIDO

LISTA DE CUADROS

Pág.

LISTA DE ANEXOS

Pág.

RESUMEN

El presente proyecto de pasantía surge a partir de la observación realizada en la Clínica San José S.A.S., cuyos activos en este caso la información, dispositivos de red, aplicaciones etc., se preservan en condiciones poco confiables, ya que no cuentan con las políticas, procedimientos, manuales, planes de contingencias formales para el resguardo de la información y la protección de la misma. La auditoría realizada se enfocó en la evaluación de la seguridad física y lógica de la infraestructura tecnológica de la empresa, bajos los aspectos de: seguridad física, seguridad lógica, infraestructura de red, servicio de mantenimiento de equipos, y base de datos.

INTRODUCCIÓN

Los cambios que se observan en el mundo moderno aumentan la tendencia de ataques informáticos a objetivos tan diversos como personas particulares o entidades financieras, acrecentando la vulnerabilidad de tales sistemas; debido a esto, las empresas han recurrido a mejorar la seguridad de sus sistemas de información, implementado controles apropiados que incluyan políticas, estructuras organizacionales y funciones que mejoren la calidad tanto de software como de hardware en sus instalaciones.

El riesgo de sufrir un ataque o una pérdida en los activos, que para el caso de las empresas sería la información manejada por ellas, es algo latente. Para esto es necesario concientizar a las entidades de proteger sus activos informáticos, con el fin de minimizar los riesgos y asegurar la continuidad del negocio.

Teniendo en cuenta toda esta situación, el objetivo de este proyecto fue realizar una auditoría informática en la Clínica San José S.A.S.; luego de realizar un diagnóstico situacional se vislumbró que era necesario realizar dicha auditoría con el fin de evaluar los posibles riesgos que pueden existir dentro de las instalaciones de la empresa.

En la primera parte del proyecto se muestra la razón por la cual fue importante realizar la evaluación de la seguridad física, lógica, infraestructura de red, servicio de mantenimiento de equipo y evaluación a la base de datos de la empresa en mención. En la segunda parte se observa una breve descripción de los conceptos de auditoría informática, la norma ISO/IEC 27001 que se implementó y las leyes que rigen la auditoría de los sistemas de información.

La tercera parte contiene la metodología con la que se llevaron a cabo todos los procedimientos empleados en el proyecto. En el cuarto capítulo se muestran los resultados y el análisis de resultados realizado durante la ejecución de la auditoría informática. Finalmente, el quinto y sexto capítulo incluyen un plan de recomendaciones para futuros trabajos y las conclusiones obtenidas.

1. EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

1.1. DESCRIPCIÓN BREVE DE LA EMPRESA Y LA DEPENDENCIA DONDE SE VA A DESEMPEÑAR.

La CLINICA SAN JOSE SAS se dedica a la prestación de servicios de salud de primer y segundo nivel de atención, esta diseña su Modelo de Atención en Salud, siguiendo los lineamientos establecido en cada uno de los procedimientos establecidos dentro del sistema de gestión de la calidad y de esta forma poner en funcionamiento la operación de la prestación de servicios de salud a la población buscando un acceso adecuado a los servicios, calidad en la atención y eficiencia en el uso de recursos y las normas vigentes en el sistema de salud.

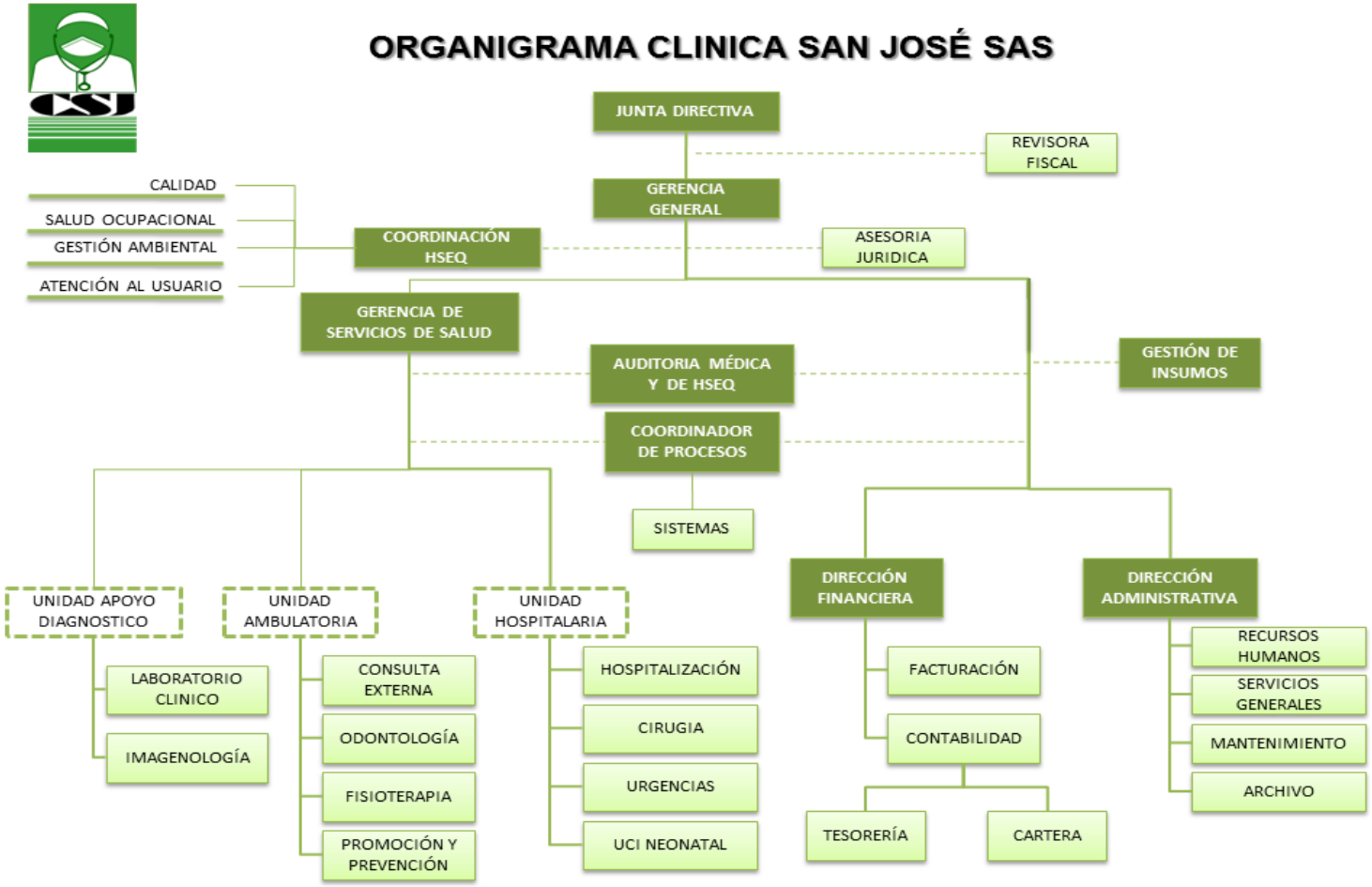
1.1.1. Misión. Prestar servicios de salud, asegurando oportunidad en la atención y calidad en el servicio; con un excelente recurso humano y las mejores condiciones tecnológicas que nos permiten cubrir con responsabilidad, eficiencia y eficacia a la comunidad de Barrancabermeja y su área de influencia, propendiendo por la calidez en la atención y el bienestar de sus usuarios.[1]

1.1.2. Visión. La clínica san José se posesionará en el próximo quinquenio, como una IPS con servicios de I, II y III nivel líder en Barrancabermeja y su área de influencia, en la prestación de servicios de salud bajo estándares de sistemas integrados de gestión, con eficiencia y eficacia de sus servicios y con la ética, responsabilidad y calidez de su entusiasta grupo de colaboradores.[2]

1.1.3. Objetivos de la empresa. La clínica San José de Barrancabermeja busca poner en funcionamiento la operación de la prestación de servicios de salud a la población obteniendo un acceso adecuado a los servicios, calidad en la atención y eficiencia en el uso de recursos y las normas vigentes en el sistema de salud, y de esta manera poder posicionarnos como una IPS servicios de I, II y III nivel líder en Barrancabermeja y su área de influencia.[3]

[1] Clínica San José S.A.S. Modelo de atención portafolio (Misión) [citado el 01 de Agosto de 2013]
[2] Clínica San José S.A.S. Modelo de atención portafolio (Visión) [citado el 01 de Agosto de 2013]
[3] Clínica San José S.A.S. Modelo de atención portafolio (Objetivo de la empresa) [citado el 01 de Agosto de 2013]

1.1.4. Descripción de la estructura Organizacional



Fuente: Clínica San José S.A.S. Modelo de atención portafolio (Organigrama)

1.1.5. Descripción de la dependencia a la que fue asignado. La Clínica San José S.A.S de la ciudad de Barrancabermeja es una entidad privada que cuenta con la prestación de servicios de salud de primer y segundo nivel de atención. El área de sistemas se encuentra adscrita al departamento de coordinación de procesos, que se encarga de administrar y controlar los recursos informáticos de hardware y software que soportan las actividades que se llevan a cabo en la empresa.

Entre otras actividades de esta dependencia se encuentran:
Soporte a usuarios
Realización de copias de seguridad
Soporte a la Red
Mantenimiento preventivo a los equipos de cómputo
Administración de servidores.[4]

1.2. DIAGNÓSTICO INICIAL DE LA DEPENDENCIA ASIGNADA.

Cuadro 1. Diagnóstico inicial

Fortalezas	**Debilidades**
La Clínica San José cuenta con un sistema integral de información en salud (SIIS). Existe una red cableada internet que permite la comunicación de todas las áreas de la empresa, contando con un proveedor de servicios. Existe una infraestructura de red con un proveedor de servicios el cual les brinda conexión a internet bajo un canal dedicado en fibra óptica de 2MB	La clínica san José no cuenta con un circuito cerrado de vigilancia las 24 horas del día. No cuenta con herramientas técnicas para las labores de mantenimiento a los equipos de cómputo. No cuenta con pararrayos en sus instalaciones.
Amenazas	**Oportunidades**
Pérdida de la información en un momento dado. Perder cobertura de la señal en la red debido a la falta de un pararrayo en la empresa). No tener soporte de la entrada y salida del personal para poder actuar en circunstancias de riesgos (robo de activos)	Optimizar la estructura de la red (LAN) para proveer múltiples cambios en el entorno. Alcanzar el tercer orden de atención. Liderazgo a nivel de atención a los clientes

Fuente. Pasante del proyecto

[4] Clínica San José S.A.S. (Modelo de atención portafolio) [citado el 01 de Agosto de 2013]

1.2.1 Planteamiento del problema. La ciudad de Barrancabermeja Santander, cuenta con clínicas que brindan la prestación de servicios en salud a sus clientes, entre las cuales se encuentra la Clínica San José S.A.S, cuyo objetivo principal es brindar la mejor atención médica a sus clientes, contando con un número considerable de médicos, cirujanos, especialistas, centros de atención etc.

La clínica San José ha mantenido una tradición de prestación de servicios en salud desde hace 15 años en la región, cuyo esfuerzo y dedicación la ha puesto como una empresa líder en el sector salud, destacándose por su excelencia en los servicios brindados y su alta calidad en la atención y eficiencia en el uso de recursos y las normas vigentes en el sistema de salud.

Actualmente, la Clínica San José maneja un número considerables de clientes por día.

En algunas ocasiones, la empresa ha tenido un cese de actividades momentáneas en su sistemas de infraestructura de red en cuanto al soporte a los equipos de cómputo se refiere (hardware), lo cual genera un descontento a sus clientes y la pérdida de tiempo para ambas partes. Es evidente además que la empresa en mención, pese a que no se ha presentado ningún inconveniente de tipo lógico o humano que pudiera poner en riesgo la seguridad de la información, no cuenta con planes de contingencia, ni informes de auditoría que evidencien la realización de evaluaciones periódicas a los recursos informáticos con los que cuenta. Por tal razón, es imperiosa la necesidad de implementar una estrategia que permita hacer un diagnóstico sobre el estado actual de sus sistemas de información.

1.3. OBJETIVOS DE LA PASANTÍA.

1.3.1. **General.** Evaluar mediante el estándar ISO 27001 de la seguridad física y lógica de la infraestructura tecnológica de la Clínica San José S.A.S de la ciudad de Barrancabermeja – Santander.

1.3.2. **Específicos.** Realizar el estudio inicial del entorno a auditar mediante la solicitud de la documentación necesaria.

Diseñar los instrumentos de recolección de información necesarios para llevar a cabo la evaluación de cada una de los aspectos de la actual auditoría.

Recolectar toda la información necesaria en cuanto a la seguridad física y lógica de las instalaciones de la Clínica se refiere.

Elaborar el Informe Final de auditoría con la evaluación realizada a cada uno de los aspectos y su respectivo Plan de Recomendaciones.

1.4. DESCRIPCIONES DE LAS ACTIVIDADES A DESARROLLAR EN LA MISMA.

Cuadro 2. Descripcion de las actividades a desarrollar en la misma

Objetivo general	Objetivos específicos	Actividades a desarrollar en la empresa para hacer posible el cumplimiento de los Objetivos específicos
Evaluar mediante el estándar ISO 27001 de la seguridad física y lógica de la infraestructura tecnológica de la Clínica San José S.A.S de la ciudad de Barrancabermeja – Santander.	Realizar el estudio inicial del entorno a auditar mediante la solicitud de la documentación necesaria.	• Evaluación de la documentación suministrada por la entidad.
	Diseñar los instrumentos de recolección de información necesarios para llevar a cabo la evaluación de cada una de los aspectos de la actual auditoría.	• Diseño de un programa que detalle las actividades que se desarrollaran durante el proceso. • Elaboración de guías de auditoría. • Elaboración de formatos de entrevistas • Diseño de cuestionarios • Diseño de Checklist de Rango • Diseño de Checklist Binario • Elaboración de formatos para verificación • Elaboración de formatos para pruebas sustantivas y de cumplimiento
	Recolectar toda la información necesaria en cuanto a la seguridad física y lógica de las instalaciones de la Clínica se refiere.	• Revisión de los cuartos de cableado y los espacios donde se encuentren los dispositivos de la red. • Análisis del sistema de cámaras de vigilancia dentro de la empresa. • Evaluación de la seguridad de los equipos (fallas en el control de temperatura o humedad), como por ejemplo robo,

Cuadro 2. (Continuación)

		incendio, inundación, interferencia eléctrica. • Revisión de las instalaciones eléctricas y de datos. • Verificación de la existencia de herramientas de gestión de seguridad. • Evaluación de las herramientas técnicas y de gestión de seguridad. • Verificación de la existencia de aplicaciones de barreras y procedimientos que resguarden el acceso a los datos. • Comprobación de las restricciones a los servicios informáticos de la entidad. Verificación de los niveles de seguridad informática.
	Elaborar el Informe Final de auditoría con la evaluación realizada a cada uno de los aspectos, y su respectivo Plan de Recomendaciones.	• Organización de los papeles de trabajo. • Tabulación de instrumentos de recolección. • Procesamiento de los datos. • Análisis de la información obtenida. • Elaboración del Informe Final de Auditoría.

Fuente: Pasante del Proyecto

1.5. ALCANCE

El presente proyecto se llevará a cabo en la Clínica San José S.A.S de la ciudad de Barrancabermeja Santander. Durante 4 meses se realizará la evaluación mediante el estándar ISO 27001 de la seguridad física, seguridad lógica, infraestructura de red, servicio de mantenimiento de equipos y de la base de datos de la empresa, desarrollando diferentes actividades que permitan analizar y verificar todos los procedimientos que se llevan a cabo en el área de sistemas, y la forma como se documenten todos estos procedimientos.

2. ENFOQUES REFERENCIALES

2.1. ENFOQUE CONCEPTUAL

2.1.1. Información[5]. La información es un conjunto de datos dispuestos de manera que nos permitan adquirir cualquier tipo de conocimiento. Asimismo, es uno de los principales activos de las organizaciones, por lo que salvaguardarla es vital para la continuidad del negocio.

2.1.2. Sistemas de Información[6]. Los Sistemas de Información (SI) son conjuntos organizados de elementos que procesan y distribuyen información con el fin de cumplir unos objetivos. No es necesario que estén basados en ordenadores. La utilización de aplicaciones informáticas sobre soportes informáticos da lugar a los Sistemas de Información Automatizados (SIA).

Los Sistemas de Información pretenden proporcionar una información oportuna y exacta para el apoyo en la toma de decisiones de la compañía. Además, garantizan la confiabilidad, la integridad y disponibilidad de la información. El uso de Sistemas de Información automatiza procesos operativos y pretenden conseguir ventajas competitivas en el mercado.

Características de los datos en un sistema de información:

Integridad. Para la Seguridad de la Información, la integridad es la propiedad que busca mantener a los datos libres de modificaciones no autorizadas.

Confidencialidad. La confidencialidad es la propiedad de prevenir la divulgación de información a personas o sistemas no autorizados.

Disponibilidad. La Disponibilidad es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones.

2.1.3 Auditoria de Sistemas de información[7]. La Auditoría de Sistemas de Información es el proceso de recoger y evaluar las evidencias para determinar la seguridad de los sistemas informáticos, la salvaguarda de los activos, la integridad de los datos y conseguir los objetivos de la organización con eficacia y con consumo de recursos eficiente.

[5] INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Security Techniques. Code of Practice for Information Security Management. Geneva: ISO/IEC, 2005, 107 P (ISOIIEC 27002:2005 (E)).

[6] Universidad Carlos III de madrid escuela politecnica superior calidad y seguridad de la información y auditoría informática

[7] Universidad Carlos III de madrid escuela politecnica superior calidad y seguridad de la información y auditoría informática

Por tanto, la Auditoría de Sistemas de Información mantiene la obtención de los objetivos de la Auditoría tradicional, que tiene como foco la salvaguarda de los activos y la integridad de los datos, y además los objetivos de eficacia y eficiencia. El proceso de la Auditoría de Sistemas de Información se puede concebir como una fuerza que ayuda a las organizaciones a conseguir mejor estos objetivos.

Importancia de realizar auditorías a los sistemas de información:

La Auditoria es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo: informática, organización de centros de información, hardware y software.

La Auditoria del Sistema de Información en la empresa, a través de la evaluación y control que realiza, tiene como objetivo fundamental mejorar la rentabilidad, la seguridad y la eficacia del sistema mecanizado de información en que se sustenta.

2.1.4 Auditoría[8]. La auditoría es un proceso sistemático que se realiza para obtener y evaluar de manera objetiva las evidencias relacionadas con informes presentados sobre acciones que tienen que ver directamente con las actividades que se desarrollan en un área o una organización, sea pública o privada.

La auditoría es un proceso sistemático. Esto quiere decir que en toda auditoría debe existir un conjunto de procedimientos lógicos y organizados que se deben cumplir para la recopilación de la información con el fin de emitir una opinión final.

Auditoría a Bases de Datos[9]. Es el proceso que permite medir, asegurar, demostrar, monitorear y registrar los accesos a la información almacenada en las bases de datos incluyendo la capacidad de determinar:

Quién accede a los datos.
Cuándo se accedió a los datos.
Desde qué tipo de dispositivo/aplicación.
Desde que ubicación en la Red.
Cuál fue la sentencia SQL ejecutada.
Cuál fue el efecto del acceso a la base de datos.

Es uno de los procesos fundamentales para apoyar la responsabilidad delegada a IT por la organización frente a las regulaciones y su entorno de negocios o actividad.

[8] FERNÁNDEZ, Eduardo. CFT soeduc concepto de auditoría Disponible en internet: <www.soeduc.cl/apuntes/concepto%20de%20auditoria.doc>
[9] En Línea http://www.jkmst.com

Auditoría a Redes de Datos[10]. Una Auditoria de Redes es, en esencia, una serie de mecanismos mediante los cuales se pone a prueba una red informática, evaluando su desempeño y seguridad, a fin de lograr una utilización más eficiente y segura de la información.

2.1.5 Controles. Conjunto de disposiciones metódicas, cuyo fin es vigilar las funciones y actitudes de las empresas y para ello permite verificar si todo se realiza conforme a los programas adoptados, órdenes impartidas y principios admitidos.

Clasificación general de los controles.

Controles Preventivos. Son aquellos que reducen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones.

Ejemplos: Letrero "No fumar" para salvaguardar las instalaciones.

Sistemas de claves de acceso

Controles detectivos. Son aquellos que no evitan que ocurran las causas del riesgo sino que los detecta luego de ocurridos. Son los más importantes para el auditor. En cierta forma sirven para evaluar la eficiencia de los controles preventivos.

Ejemplo: Archivos y procesos que sirvan como pistas de auditoría

Procedimientos de validación

Controles Correctivos. Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en si una actividad altamente propensa a errores.

2.1.6 Estándar ISO/IEC 27001[11]. Es un estándar para la seguridad de la información (Information technology - Security techniques - Information security management systems

Requirements) aprobado y publicado como estándar internacional en octubre de 2005 por International Organization for Standardization y por la comisión International Electrotechnical Commission.

Especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) según el conocido como

[10] DEL PESO NAVARRO, EMILIO; DEL PESO, MAR; PIATTINI VELTHUIS, MARIO G. (2008). Auditoría de Tecnologías y Sistemas de Información
. México: Alfaomega Ra-Ma.

[11] Estándar Internacional ISO 27001. Tecnologia de la información – Tecnicas de seguridad –Sistemas de gestión de seguridad de la información- Requerimiento

"Ciclo de Deming":PDCA - acrónimo de Plan, Do, Check, Act (Planificar, Hacer, Verificar, Actuar). Es consistente con las mejores prácticas descritas en ISO/IEC 27002, anteriormente conocida como ISO/IEC 17799, con orígenes en la norma BS 7799-2:2002, desarrollada por la entidad de normalización británica, la British Standards Institution (BSI).

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

Este proceso es el que constituye un Sistema de Gestión de Seguridad de la Información SGSI, que podría considerarse, por analogía con una norma tan conocida como ISO 9001, como el sistema de calidad para la seguridad de la información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Seguridad de la información[12]. Según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

Confidencialidad. La información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

Integridad. Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad. Acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Cuatro fases del sistema de gestión de seguridad de la información[13]. La norma ISO 27001 determina cómo gestionar la seguridad de la información a través de un sistema de gestión de seguridad de la información. Un sistema de gestión de este tipo, igual que las normas ISO 9001 o ISO 14001, está formado por cuatro fases que se deben implementar en forma constante para reducir al mínimo los riesgos sobre confidencialidad, integridad y disponibilidad de la información.

[12] Auditoría de Sistemas de Información. Seguridad informática: Conceptos básicos, Capítulo 1 [en línea] Disponible en Internet: <http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf>
[13] Disponible en línea http://www.iso27001standard.com

Las fases son las siguientes:

La Fase de planificación. Esta fase sirve para planificar la organización básica y establecer los objetivos de la seguridad de la información y para escoger los controles adecuados de seguridad (la norma contiene un catálogo de 133 posibles controles).

La Fase de implementación. Esta fase implica la realización de todo lo planificado en la fase anterior.

La Fase de revisión. El objetivo de esta fase es monitorear el funcionamiento del SGSI mediante diversos "canales" y verificar si los resultados cumplen los objetivos establecidos.

La Fase de mantenimiento y mejora. El objetivo de esta fase es mejorar todos los incumplimientos detectados en la fase anterior.

El ciclo de estas cuatro fases nunca termina, todas las actividades deben ser implementadas cíclicamente para mantener la eficacia del SGSI.

2.1.7. Análisis de riesgos informáticos[14]. El análisis del riesgo es un método sistemático de recopilación, evaluación, registro y difusión de información necesaria para formular recomendaciones orientadas a la adopción de una posición o medidas en respuesta a un peligro determinado. Hay pequeñas variaciones en la terminología utilizada por las tres organizaciones. Sin embargo, las tres organizaciones hermanas consideran el análisis del riesgo como un proceso que consta de cuatro etapas:

Identificación del peligro;
Evaluación del riesgo;
Gestión del riesgo; y
Comunicación del riesgo.

La **identificación del peligro** consiste en especificar el acontecimiento adverso que es motivo de preocupación.

En la **evaluación del riesgo** se tiene en cuenta la probabilidad (la probabilidad real y no sólo la posibilidad) de que se produzca el peligro, las consecuencias si ocurre y el grado de incertidumbre que supone. (Obsérvese que esta descripción de la evaluación del riesgo es diferente de la definición que figura en el Acuerdo MSF.)

La **gestión del riesgo** consiste en la identificación y aplicación de la mejor opción para reducir o eliminar la probabilidad de que se produzca el peligro.

[14] Disponible en Linea http://www.wto.org

La **comunicación del riesgo** consiste en el intercambio abierto de información y opiniones aclaratorias que llevan a una mejor comprensión y adopción de decisiones.

2.2. ENFOQUE LEGAL

El presente trabajo tiene como base legal las siguientes normas

Ley 1273 DE 2009[15]. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado de la protección de la información y de los datos y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

EL CONGRESO DE COLOMBIA Decreta:

ARTÍCULO 1°. Adiciónese el Código Penal con un Título VII BIS denominado "De la Protección de la información y de los datos.

De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos

Artículo 269ª: **Acceso abusivo a un sistema informático**.

El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269C: **Interceptación de datos informáticos**.

El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: **Daño Informático**.

El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

[15] Constitución política de Colombia. De la protección de la información y de los datos, Ley 1273 de 2009 [En Línea] Disponible en internet: <http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.htm>

Artículo 269F: **Violación de datos personales**.

El que, sin estar facultado para ello, con provecho propio o 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 o medios semejantes, 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.

2.2.1 Convenio Institucional. Convenio marco de apoyo Interinstitucional para la realización de pasantías y/o prácticas profesionales, celebrado entre la Universidad Francisco de paula Santander seccional Ocaña y la Clínica San José S.A.S.

3. INFORME DE CUMPLIMIENTO DE TRABAJO

3.1. PRESENTACIÓN DE RESULTADOS

3.1.1 Generalidades. Para realizar la evaluación de la seguridad física y lógica de los sistemas de información de la Clínica San José S.A.S., se utilizó el estándar ISO/IEC 27001: Sistema de Gestión de Seguridad de la Información bajo los siguientes aspectos: Seguridad Física, Seguridad Lógica, Servicio de Mantenimiento de Equipos, Infraestructura de Red y Evaluación a La Base de Datos.

3.1.2 Evaluación mediante el estándar ISO 27001 de la Seguridad Física y Lógica de la infraestructura tecnológica de la Clínica San José S.A.S de la ciudad de Barrancabermeja – Santander. Para llevar a cabo la evaluación de la Seguridad Física y Lógica de la infraestructura tecnológica de la Clínica San José S.A.S, se llevaron a cabo las siguientes actividades:

Recolección de información primaria. Para dar inicio al proceso de auditoria se aplicó una entrevista al gerente de la Clínica San José S.A.S para definir el objeto y delimitar los aspectos de la auditoria. (Ver Anexo F)

Para llevar a cabo esta actividad, se hizo necesario realizar un Plan de auditoría que contempló el diseño de las actividades que se llevarían a cabo en cada etapa del proceso. Dichas actividades, se relacionan a continuación:

Evaluación de la documentación suministrada por la entidad. Al iniciar labores dentro de la Clínica San José S.A.S. se realizó un oficio el cual fue dirigido al Gerente de la clínica solicitando la información pertinente para realizar el estudio del entorno a auditar. (Ver Anexo A)

También se presentó otra solicitud al Coordinador de Procesos de la Clínica para obtener información del área de sistemas. (Ver Anexo B)

De toda esta información solo recibí la siguiente: (Ver Anexo C)

Filosofía Institucional de la Empresa
Organigrama de la Empresa
Programas de mantenimiento de equipos de cómputo
Manual de usuario de las aplicaciones
Procedimientos formales de realización de copias de seguridad

3.1.3 Diseño de un Plan que detalle las actividades que se desarrollaron durante el proceso.

Diseño del Plan de Auditoría. El Plan de Auditoría para la presente evaluación de la Seguridad Física y Lógica de la Clínica San José S.A.S. se relaciona en el Anexo D.

Elaboración de Guías de Auditoría. Las guías de auditoría se utilizaron para hacer un seguimiento y un control sobre las actividades a desarrollar en cada una de las fases del proceso, para dar cumplimiento a los objetivos trazados. **(**Ver Anexo E)

Recolección de información secundaria. Para obtener la segunda fuente de información se hizo necesario utilizar los siguientes instrumentos:

EVALUACIÓN DE LA SEGURIDAD FÍSICA. En primera instancia, se aplicó una Entrevista al Coordinador de Procesos encargado del área, y se evaluó mediante un Checklist de Rango. (Ver Anexos G y G1)

Para complementar la información relacionada con factores ambientales, se aplicó una Entrevista al Jefe de Mantenimiento y se evaluó mediante un Checklist de Rango.
(Ver Anexos H y H1)

EVALUACIÓN DE LA SEGURIDAD LÓGICA. Para evaluar este aspecto, en primera medida, se hizo necesario realizar un inventario de las aplicaciones de software instaladas en los diferentes equipos que le dan soporte a los servicios ofrecidos por La Clínica San José S.A.S. (Ver Anexo I.)

En segunda instancia, se aplicó una Entrevista al Coordinador de Procesos encargado del área, y se evaluó mediante un Checklist de Rango (Ver Anexo J y J1)

EVALUACIÓN AL SERVICIO DE MANTENIMIENTO DE EQUIPOS. Para evaluar dicho servicio, se aplicó una Entrevista al Coordinador de Procesos encargado del área, y se evaluó mediante un Checklist de Rango (Ver Anexo K y K1)

EVALUACIÓN A LA INFRAESTRUCTURA DE RED DE DATOS. Se utilizó un Checklist binario, aplicado al Coordinador de Procesos encargado del área (Ver Anexo L):

EVALUACIÓN A LA BASE DE DATOS. Inicialmente, se aplicó una entrevista al administrador de la base de datos para obtener información vital para todo el proceso de análisis de las tablas maestras, de acuerdo con el siguiente formato (Ver Anexo M).

En segunda medida, se aplicó una evaluación a la Base de Datos, con el fin de identificar vulnerabilidades técnicas del Sistema de Gestión de Bases de Datos (DBMS), utilizando los siguientes formatos. Se hace la salvedad que la Clínica San José S.A.S., cuenta con un sistema de información integral en salud SIIS, con un motor de base de datos en PostgreSQL donde se llevando todos los procedimientos que realiza la empresa a diario.

Cuadro 3. Consulta de Duplicados

Consulta	**Duplicados**
Objetivo	Verificar integridad de los datos

Cuadro 3. (Continuación)

Campos	Nombre de los atributos de la tabla		
Tabla	Registros	Resultado	Comentarios

Fuente: Pasante del Proyecto

Cuadro 4. Consulta de Campos Nulos

Consulta	**Campos nulos**		
Objetivo	Verificar integridad de los datos		
Campos	Nombre de los atributos de la tabla		
Tabla	Registros	Resultado	Comentarios

Fuente: Pasante del Proyecto

Cuadro 5. Verificar Campos tipo fecha

Consulta	**Verificar Campos tipo fecha (Operador Between)**		
Objetivo	Determinar límites correctos. Verificar integridad de los datos		
Campos	Nombre de los atributos de la tabla		
Tabla	Registros	Resultado	Comentarios

Fuente: Pasante del Proyecto

El procesamiento de dicha información, se puede ver en el Anexo N.

Verificación de la información recolectada. Después de haber aplicado los instrumentos de recolección de información, se procedió a verificar la información obtenida, para lo cual se diseñaron dos formatos así:

VERIFICACIÓN DE LA SEGURIDAD FÍSICA. Se utilizó la técnica de observación para corroborar la información recolectada con anterioridad. Dicha confirmación se hizo a través del formato mostrado en el Anexo Ñ.

VERIFICACIÓN DE LA SEGURIDAD LÓGICA. Se utilizó la técnica de observación para corroborar la información recolectada con anterioridad. Dicha confirmación se hizo a través del formato mostrado en el Anexo O.

3.1.4 Resultados de la Auditoría. Una vez realizado todo el proceso de estudio, recolección y verificación de información se obtuvieron los siguientes resultados en cada uno de los aspectos evaluados, de acuerdo con el estándar ISO/IEC 27001[16]

SEGURIDAD FÍSICA

Alcances

Controles físicos de entrada
Seguridad de oficinas, habitaciones e instalaciones
Protección contra amenazas externas y ambientales
Ubicación y protección del equipo
Seguridad del cableado
Mantenimiento de equipos
Planes de contingencias.

Hallazgos Potenciales.

Después de haber evaluado este aspecto, se pudo determinar que:

La empresa cuenta con un sistema de refrigeración con aire acondicionado, instalados en cada una de las áreas que comprenden el interior de la entidad auditada.
La entidad cuenta con extintores en caso de alertas de incendios
La Clínica cuenta con un sistema alterno de suministro de energía eléctrica
Cuenta con salidas de emergencias
A pesar que existe un servicio de vigilancia privada, algunas áreas críticas como el área de sistemas, no poseen controles de acceso físico a las mismas, lo que puede causar pérdida parcial o total tanto de activos físicos como de información.
Buena calidad del cableado
La clínica cuenta con sistema de bomba sumergible
La clínica posee un equipo de conexión a tierra
No existen alarmas contra incendios
La empresa no posee detectores de humo
La empresa cuenta con cámaras de vigilancia, pero estas se encuentran cumpliendo solo la función de visualización, más no de grabación, lo que pone en riesgo la seguridad de los activos de la entidad.
No cuentan con cámaras de vigilancia al exterior de la empresa
Existe una conexión polo a tierra en general
El cableado de datos no es independiente del cableado de corriente
Se tiene un inventario de los equipos que soportan la red de datos de la empresa
Existe un medidor de temperatura para el rack de comunicaciones
No existen medidas de seguridad física para las copias de respaldo
No existen planos de red

[16] Diseño de un sistema de gestión de SEGURIDAD D INFORMACION Óptica ISO 27001

No se tiene un plan de contingencias documentado
No se cuenta con un pararrayos que proteja los dispositivos que soportan la red de datos
No se realizan bitácoras de los procedimientos operativos realizados a diario por el área de sistemas

Conclusiones

La Seguridad Física en el ámbito informático de la Clínica San José S.A.S., a pesar que cuenta con procedimientos de seguridad para la mayoría de los recursos informáticos, carece de políticas formales que permitan implementar medidas de protección para los mismos de acuerdo con lo establecido en el estándar internacional ISO/IEC 27001 en el debido cumplimiento de las Normas de seguridad.

Recomendaciones

Implementar un mecanismo de alarma contra incendios
Poner en total funcionamiento el circuito cerrado de televisión
Implementar un sistema de vigilancia al exterior de la Clínica
Separar todo el cableado de datos del cableado eléctrico
Reubicar las copias de respaldo físicas fuera de las instalaciones de la empresa
Diseñar planos de red
Elaborar un plan de contingencias de sistemas de información y capacitar al personal para su adecuada implementación.
Disponer de un sistema ante descargas eléctricas (Pararrayos)
Utilizar bitácoras para los procedimientos realizados por el personal de sistemas, en cada una de las áreas a las que brinda soporte técnico.

SEGURIDAD LÓGICA

Alcances

Políticas de control de accesos
Registro de usuarios
Gestión de privilegios
Políticas de escritorios y pantallas limpias
Seguridad de la información.
Control del software operativo
Políticas de control de cambios
Licencias de software
Copias de respaldo.

Hallazgos Potenciales

Luego de haber evaluado este aspecto se pudo obtener lo siguiente:

Existen restricciones para el acceso a los equipos de cómputo a través de contraseñas
Se cuenta con un software de antivirus actualizado (AVAST)
La empresa cuenta con un servidor proxy llamado IPCop.
Existe un programa de recuperación de archivos en versión Free llamado Hiren's Boot
Existen restricciones a la base de datos
Se tiene licencia de software corporativa (Office Profesional 2010)
Se realizan copias de respaldo
Existe un formato de registro de copias de respaldo
No se cuenta con un software anti espía
No se tiene en la empresa una política que establezca un acuerdo de confidencialidad de documentos
No existen políticas para la seguridad de la información
La empresa no cuenta con pólizas contra robos
No existen pólizas contra incendios
No se realizan auditorias periódicas a los medios de almacenamientos

Conclusiones

La Clínica a pesar que vela por la seguridad de la información utilizando herramientas que le permitan la protección de esta, tiene falencias en cuanto a procedimientos formales y políticas previamente establecidas que le permitan un normal desempeño en sus actividades diarias.

Recomendaciones:

Implantar políticas de seguridad de la información, documentarlas e implementarlas, de acuerdo como lo establece la norma ISO/IEC 27001.
Implementar software anti espía
Establecer una póliza que contemple acuerdos de confidencialidad de la información al momento de ser contratado
Implementar pólizas contra robos en los activos
Adquirir pólizas contra incendios
Llevar un seguimientos bajo auditorias periódicas a los medios de almacenamiento

SERVICIO DE MANTENIMIENTO DE EQUIPOS DE CÓMPUTO

Alcances

Planes y procedimientos de Mantenimiento.
Tiempos de respuesta
Inventario de equipos de cómputo

Hallazgos Potenciales

Luego de haber evaluado este aspecto se pudo obtener lo siguiente:

Realización de mantenimientos preventivos a los equipos de cómputo
Procedimientos inmediatos de atención a la notificación de cualquier evento irregular en el funcionamiento de los equipos de cómputo
Inventario actualizado
No se cuenta con seguros contra robo para los equipos de cómputo
No existe una política que contemple la adquisición de nuevos equipos
No existe una política que exija la verificación de los mantenimientos preventivos
No existe una política que contemple los equipos en garantía
No existe una póliza de seguros para la protección de los equipos de cómputo

Conclusiones

El servicio de mantenimiento de equipos de cómputo de la Clínica se encuentra en buen estado, ya que cuenta con procedimientos inmediatos de atención a la notificación de cualquier evento irregular en el funcionamiento de los mismos, lo que hace que los servicios soportados por dichos equipos de cómputo sean eficientes. Sin embargo, se evidenció, la carencia de procedimientos formales de protección de equipos.

Recomendaciones

Implementar seguros contra robos
Diseñar e implementar políticas para la adquisición de nuevos equipos
Establecer políticas de verificación de los mantenimientos preventivos
Establecer política para los equipos en garantía
Adquirir póliza de seguros para los activos de la empresa

INFRAESTRUCTURA DE RED DE DATOS

Alcance

Políticas de utilización de los servicios de red
Identificación de equipos en redes
Control de conexión de redes
Control de direccionamiento en la red

Hallazgos Potenciales

Luego de haber evaluado este aspecto se pudo obtener lo siguiente:

La clínica cuenta con un cuarto de comunicaciones
Se tiene Switch adicionales en caso de fallas
Existe una separación entre el cuarto de telecomunicaciones y los equipos de computo
La red cuenta con direccionamiento con IP fijas e IP dinámicas
Se tiene UPS para la protección de los equipos

Existe un canal dedicado de 2 MB en fibra óptica
Existe restricción de acceso a los router
La red está Protección contra intrusos
Existe la herramienta necesaria para el montaje de la Red
No existe una etiquetación de nodos para reducción de velocidad de transmisión
El cableado de la empresa no está certificado
El armario del cableado no cumple con los estándares de red
No se encuentra implementado un mapa de sembrado de nodos
No existe un mapa de rutas de red
No se cuenta con una red específica para la transmisión de datos, voz y video
El cableado no viaja en canaletas o ductos
No se cuenta con la última categoría del cableado UTP
No existe un registro formal de eventos para los usuarios que acceden a la red
No existe una separación del cableado de datos con el de transmisión de corriente

Conclusiones

A nivel de infraestructura de la red de datos, se puede concluir que la clínica tiene implementados algunos mecanismos de seguridad física y lógica que permiten mantener un cierto grado de confidencialidad de la información que viaja o se transmite a través de la red de datos y para dar soporte a los servicios ofrecidos por la clínica.

Por su parte, la evaluación de dicho aspecto a través del Checklist binario, permite evidenciar que aquellos ítems marcados con **NO** (Ver Anexo L) corresponden a aspectos negativos que pueden poner en riesgo la seguridad, integridad y disponibilidad de la información.

Recomendaciones

Reestructurar el rack de comunicaciones
Realizar e implementar un mapa de red
Implementar la separación del cableado de datos y el de corriente
Implementar canaletas para el transporte del cableado
Establecer una política que contemple el registro formal de eventos para el acceso a la red de datos.

BASE DE DATOS

Alcance

Validación de datos de entrada
Control de procedimiento interno
Validación de los datos de salida
Integridad, Confidencialidad y Disponibilidad de la información

Hallazgos Potenciales

Duplicidad de los datos
Falta de controles de validación de los datos de entrada al sistema
Falta de integridad de los datos
Se evidencia que no existe una renovación de clave de usuarios ni cambios de estas de forma automática.

Conclusiones

A nivel de base de datos la Clínica San José S.A.S se encuentra de la siguiente manera:

Se realizó una serie de análisis y consultas donde se evidenció la duplicidad de la información, haciendo la salvedad que no todas las tablas contienen datos duplicados, a continuación veremos las tablas afectadas.

Se encontraron duplicados de datos en la tabla **inv_xxx_xxx_anatofarmacologico,** donde se está repitiendo el cod_anatomofarmacologico 2 veces con diferente descripcion.

En la tabla maestra **terxxxxx** existe un paciente_id que se está repitiendo con el mismo número de documento, pero con diferente tipo_id_paciente, no obstante su fecha de nacimiento es en el 2004-12-12 lo cual indica que ese paciente es menor de edad y no debe aparecer su tipo_id_paciente en Cedula de Ciudadanía. De lo cual se puede inferir que no existe integridad de los datos, ni veracidad de la información.

Se auditó la tabla paciente, la cual no está dentro del listado de tablas maestras que el administrador de base de datos de la Clínica San José S.A.S., brindó como información vital para el proceso de auditoría y se encontraron las siguientes anomalías:

Duplicidad de información, Un paciente aparece con un mismo número de identidad pero con tres (3) tipos de documentos.

Se llevó a cabo un análisis y consultas de campos nulos para verificar la integridad de los datos. Para este tipo de consultas en estado null la base de datos de la Clínica San José no posee en sus tablas maestras campo de vital importancia en estado nulo, campos como por ejemplo **numero_orden_id, txxxxxx_id, grupo_xxxxxxxxx_id**, es decir, campos donde su llave primaria este en estado Nulo.

Sin embrago existen campos que se encuentran es estado Nulo, pero estos campos no son de vital importancia a la hora de emitir un resultado o una petición, como por ejemplo:
Segundo nombre, segundo apellido, teléfono.

Se verificó el operador Between para los campos tipo fecha con el fin de determinar limites correctos, dichos resultados fueron positivos puesto que el motor de base de datos de la

Clínica San José S.A.S ejecuta las consultas y genera un reporte de las fechas solicitadas para cada procedimiento en mención.

Recomendaciones

Revisión del modelo de base de datos MER
Documentar todos los cambios y procedimientos que se realicen a nivel de software para la aplicación SIIS
Implementar las copias de seguridad automáticas para bases de datos o el almacenamiento de las mismas en la Nube.
Implementar políticas de seguridad para la base datos
Elaborar un procedimiento para dar de alta y bajas a los usuarios
Utilizar normas internacionales de la ISO/ IEC 27001 con el fin de estandarizar los niveles de seguridad para la Clínica.
La creación de un procedimiento para la continuidad de negocio tomando como base la ISO/IEC 27001.

3.1.4. Plan de Recomendaciones

Evaluación del riesgo.

De acuerdo con el estándar ISO/IEC 27001 se tiene:

Proceso de Valuación del Riesgo

El cálculo de los riesgos de seguridad de información incluye normalmente el análisis y la evaluación del riesgo. El análisis del riesgo contempla:

Identificación de Activos de información.
Tasación de los activos identificados, considerando los requerimientos legales y comerciales, así como los impactos resultantes de una pérdida por confidencialidad, integridad y disponibilidad.
Identificación de amenazas y vulnerabilidades para cada activo previamente identificado
Cálculo de posibilidades de que las amenazas y vulnerabilidades ocurran.

De acuerdo con el estándar ISO/IEC 27001 el análisis del riesgo contempla lo siguiente.

Análisis del Riesgo

Identificación de Activos

Los activos de información en la empresa, dentro del alcance del SGSI, son fundamentalmente para una correcta implementación de un SGSI.

El análisis y la evaluación del riesgo y las decisiones que se tomen en relación con el tratamiento del riesgo en la empresa giran alrededor de los activos de información identificados.

Un activo es algo que tiene valor o utilidad para la organización, sus operaciones comerciales y su continuidad. Por esta razón, los activos necesitan tener protección para asegurar una correcta operación del negocio y una continuidad en las operaciones. Para cualquier tipo de empresa son de vital importancia la gestión y la responsabilidad por los activos.

En este punto es importante clasificar qué es un activo de información en el contexto de ISO 27001:2005. Según el ISO 17799:2005 (Código de Prácticas para la Gestión de Seguridad de la Información), un activo de información es:

"Algo a lo que una organización directamente le asigna un valor y, por lo tanto, la organización debe proteger".
El ISO 17799:2005 clasifica los activos de información en las categorías siguientes

Activos de información
Documentos del papel
Activos de software
Activos físicos
Personal
Imagen de la compañía y reputación
Servicios

Identificación de Activos[17].

Activos de Información

Datos
Manual de usuario sistema de información integral en salud **SIIS** (IPSOF)
Lista de contactos
Licencias de software

Documentos de papel

Contratos
Certificaciones
Facturas

Activos de Software

[17] Diseño de un sistema de gestión de SEGURIDAD DE INFORMACIÓN Óptica ISO 27001.

Aplicación SIIS
Firewall IPCop
Software Contable JALT
Base de Datos
Correo electrónico

Activos Fisco

Computadores de escritorio
Portátiles
Impresoras
Cámaras de vigilancia
Disco duro
Servidores
Aires Acondicionados
Líneas telefónicas
Cableado de datos
Conexión eléctrica
Herramientas de mantenimiento
Router
Switch
Access Point
DVR
UPS
Estabilizadores
Planta de energía
Rack de comunicaciones
Modem

Personal

Pacientes
Trabajadores
Proveedores

Servicios

Atención al cliente
Urgencias
Hospitalización
Laboratorio
Inyecto logia

Cirugía
UCI
Apoyo a diagnostico
Centro ambulatorio
Odontología
Pediatría
Ginecología

Tasación de Activos. La tasación de activos es un factor muy importante en la evaluación del riesgo. La tasación es la asignación apropiada en términos de la importancia que éste tenga para la empresa. Para ello se deberá aplicar una escala de valor a los activos y de esa manera poder relacionarlos apropiadamente.

En este caso se tasó su impacto con relación a su confidencialidad, integridad y disponibilidad. Se estableció utilizar la escala cualitativa de: Alto, Mediano y Bajo.

Cuadro 6. Tasación de Activos

ACTIVO DE INFORMACIÓN	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	TOTAL
Aplicación SIIS	5	4	4	**4**
Firewall IPCop	5	4	3	**4**
Software Contable JALT	5	5	4	**5**
Computadores	3	3	3	**3**
Impresoras	3	3	3	**3**
Servidor de bases de datos	3	5	5	**4**
Copias de respaldo	5	5	4	**5**
Cámaras de vigilancia	3	3	3	**3**
Disco duro	5	5	4	**5**
Aires acondicionados	3	3	3	**3**
Líneas telefónicas	3	3	3	**3**
Cableado de datos	3	4	4	**4**
Conexión eléctrica	4	3	3	**3**
Herramientas de mantenimiento	3	3	3	**3**
Router	4	4	4	**4**
Switch	4	4	4	**4**
Access Point	3	3	3	**3**
DVR	3	3	3	**3**
UPS	3	3	3	**3**

Cuadro 6. (Continuación)

Estabilizadores	3	3	3	**3**
Planta de energía	4	3	3	**3**
Rack de comunicaciones	4	5	5	**5**
Modem	3	3	3	**3**
Documentos	5	5	5	**5**
Datos	4	4	4	**4**
Correo electrónico	3	3	3	**3**

Fuente: Pasante del Proyecto

PROPIETARIOS DE ACTIVOS

Cuadro 7. Propietarios de Activos

ACTIVOS DE INFORMACIÓN	PROPIETARIO
1. Aplicación SIIS	Sistemas
2. Firewall IPCop	Sistemas
3. Software Contable JALT	Contabilidad
4. Dispositivos de red	Sistemas
5. Copias de respaldo	Sistemas
6. Aires acondicionados	Área de mantenimiento
7. Líneas telefónicas	Área de mantenimiento
8. Documentos	Administración
9. Datos	Administración
10. Correo electrónico	Sistemas

Fuente: Pasante del Proyecto

Identificación de Amenazas y Vulnerabilidades. En las organizaciones, los activos de información están sujetos a distintas formas de amenazas. Una amenaza puede causar un incidente no deseado que puede generar daño a la organización y a sus activos.
"Una amenaza es la indicación de un potencial evento no deseado".

(Alberts y Dorofee, 2003). En esta definición, los autores se refieren a una situación en la cual una persona pudiera hacer algo indeseable o una ocurrencia natural. En su libro *Información Security Risk Análisis* (Walter, 2001), Thomas Welter plantea que una amenaza puede significar muchas cosas, depende del contexto en donde se le ubique.

"Una amenaza es normalmente vista como un intento de hacer algo malo a alguien o a algo" (Walter, 2001).

AMENAZAS

AMENAZAS NATURALES

Inundaciones
Incendios forestales

AMENAZAS A INSTALACIONES

Fuego
Caída de energía
Daño de agua
Fallas mecánicas

AMENAZAS HUMANAS

Epidemias
Problemas de transporte
Perdida de personal clave

AMENAZAS TECNOLÓGICAS

Virus
Hacking
Perdida de datos
Fallas de hardware
Fallas de software
Fallas en la red
Fallas en líneas telefónicas

AMENAZAS OPERACIONALES

Crisis Financiera
Falla en los equipos
Aspectos regulatorios

AMENAZAS SOCIALES

Motines
Protestas
Vandalismo

VULNERABILIDADES

Las vulnerabilidades son debilidades de seguridad asociada con los activos de información de una organización.

"Es una debilidad en el sistema, aplicaciones o infraestructura, control o diseño de flujo que puede ser explotada para violar la integridad del sistema" (Peltier, 2001).

"Las vulnerabilidades organizacionales son debilidades en las políticas organizacionales o prácticas que pueden resultar en acciones no autorizadas" (Albert y Dorofee, 2003).

Al tratar de definir las vulnerabilidades, la mejor manera es pensar en las debilidades del sistema de seguridad. Las vulnerabilidades no causan daño, Simplemente son condiciones que pueden hacer que una amenaza afecte un activo.

Las vulnerabilidades pueden clasificarse como:

SEGURIDAD DE LOS RECURSOS HUMANOS

Falta de entrenamiento en seguridad
Carencia de toma de conciencia en seguridad
Falta de políticas para el uso correcto de las telecomunicaciones
Carencia de procedimientos que asegure la entrega de los activos al término del contrato

CONTROL DE ACCESO

Falta de políticas sobre escritorio y pantalla limpia
Falta de protección al equipo de comunicación móvil

SEGURIDAD FÍSICA Y AMBIENTAL

Control de acceso físico inadecuado a oficinas
Carencia de programas para sustituir equipo.

MANTENIMIENTO, DESARROLLO Y ADQUISICION DE SISTEMAS DE INFORMACION

Carencia de validación de datos procesados
Carencia de ensayos de software.

Cálculo de las Amenazas y Vulnerabilidades. Una vez identificadas las amenazas y vulnerabilidades es necesario calcular la posibilidad de que puedan juntarse y causar un riesgo. El riesgo se define como "La posibilidad (de) que una amenaza pueda explotar una vulnerabilidad en particular" (Peltier, 2001).

Todo este proceso incluye calcular la posibilidad de la ocurrencia de amenazas y qué tan fácil pueden ser explotadas las vulnerabilidades por las amenazas.

A: Alto
M: Medio
B: Bajo

A continuación se ilustrara la tabla con el cálculo de amenazas y vulnerabilidades.

Cuadro 8. Cálculo de las amenazas y vulnerabilidades

Activo	Amenazas	Probabilidad Ocurrencia	Vulnerabilidad	Posible Explotación de vulnerabilidad
Firewall IPCop	Perdida de Datos Fallas de hardware Fallas de Software Fallas en la Red	A M M A	-Falta de protección de los backup's. -Falta de monitoreo al equipo -Carencia de ensayos de software -Reestructuración de la red	A A M A
Disco Duro	Perdida de Datos Fallas de hardware Falla en los equipos	A M M	-Falta de protección de los backup's. -Falta Políticas de manejo de activos de información -Demora en el mantenimiento preventivo	A M A
Computadores	Virus Fallas de Hardware	M M	-Mala utilización del antivirus -Demora en el mantenimiento preventivo	M A
Cableado de datos	Mal diseño Incumplimiento de las normas de instalación de la red	M A	-Reestructuración de la red -Mala segmentación del tráfico de red y la longitud máxima de cada	M A

Cuadro 8. (Continuación)

			segmento de red no es la adecuada	
Router	Desgaste Fallas de hardware	A M	-Uso constante de dispositivos, lo cual reduce el óptimo rendimiento del mismo - Poco monitoreo a estos dispositivos	A M
Access Point	Fallas de Hardware	M	-Poco monitoreo a estos dispositivos	A
Copias de respaldo	Perdida de datos	A	-Falta de mecanismos de resguardo de la información	A
Estabilizadores	Caída de energía	B	-Poco mantenimiento preventivo	B
Herramientas de mantenimiento	Robo Sabotaje	M B	-Ninguna restricción para el área de sistemas -Ninguna política sobre manipulación de herramientas	M B
Aplicación SIIS	Perdida de datos	A	-Falta de protección de los backup’s	A
Impresoras	Fallas de Hardware	M	-Demora en los mantenimientos	M

Fuente: Pasante del Proyecto

Evaluación del Riesgo. El objetivo del análisis de riesgo es identificar y calcular los riesgos basados en la identificación de los activos, y en el cálculo de las amenazas y vulnerabilidades.

Los riesgos se calculan de la combinación de los valores de los activos, que expresan el impacto de pérdidas por confidencialidad, integridad y disponibilidad y del cálculo de la posibilidad de que amenazas y que vulnerabilidades relacionadas se junten y causen y incidente.

La organización debe decidir el método para hacer el cálculo del riesgo que sea más apropiado para la empresa y los requerimientos de seguridad. Los niveles de riesgos calculados proveen un medio para poder priorizar los riesgos e identificar aquellos otros riesgos que son más problemáticos para la organización.

"Existen diferentes maneras de relacionar los valores asignados a los activos y a aquellos asignados a las vulnerabilidades y amenazas para así obtener mediciones del riesgo" (Sheffi, 2005).

Para calcular el nivel de riesgo, se hizo necesario utilizar la siguiente matriz:

Cuadro 9. Matriz de riesgo

ACTIVOS	TASACIÓN				AMENAZAS	PROBABILIDADE OCURRENCIA	VULNERABILIDAD	POSIBLE EXPLOTACIÓN DE VULNERABILIDAD	VALOR ACTIVO	POSIBLE OCURRENCIA	TOTAL RIESGO
	Confidencialidad	Integridad	Disponibilidad	Total							
Firewall IPCop	A	M	B	M	-Perdida de Datos	A	-Falta de protección de los backup's.	A	M	A	A
					-Fallas de hardware	M	-Falta de monitoreo al equipo	A	M	M	M
					-Fallas de Software	M	-Carencia de ensayos de software	M	M	B	M
					-Fallas en la Red	A	Reestructuración de la red	A	M	A	A
Disco Duro	A	A	M	A	Perdida de Datos	A	-Falta de protección de los backup's.	A	A	A	A
					Fallas de hardware	M	-Falta Polnicas de manejo de activos de información	M	A	M	M
					Falla en los equipos	M	-Demora en el mantenimiento preventivo	A	A	M	A
Computadores	B	B	B	B	Virus	M	-Mala utilización del antivirus	M	B	B	B
					Fallas de Hardware	M	-Demora en el mantenimiento preventivo	A	B	M	M
Cableado de datos	B	M	M	M	Mal diseño	M	-Reestructuración de la red	M	M	A	M
					Incumplimiento de las normas de instalación de la red	A	-Mala segmentación del trafico de red y la longitud maxima de cada segmento de red no es la adecuada	A	M	A	A
Router	M	M	M	M	Desgaste	A	-Uso constante de dispositivos, lo cual reduce el optimo rendimiento del mismo	A	M	A	A
					Fallas de hardware	M	- Poco monitoreo a estos dispositivos	M	M	M	M
Access Point	B	B	B	B	Fallas de Hardware	M	-Poco monitoreo a estos dispositivos	A	B	M	M
Copias de respaldo	A	A	M	A	Perdida de datos	A	-Falta de mecanismos de resguardo de la información	A	A	A	A
Estabilizadores	B	B	B	B	Caida de energia	B	-Poco mantenimiento preventivo	B	B	M	B
Herramientas de mantenimiento	B	B	B	B	Robo	M	-Ninguna restricción para el area de sistemas	M	B	A	M
					Sabotaje	B	-Ninguna política sobre manipulación de herramientas	B	B	B	B
Aplicación SIIS	A	M	M	M	Perdida de datos	A	-Falta de protección de los backup's	A	M	A	A
Impresoras	B	B	B	B	Fallas de Hardware	M	-Demora en los mantenimientos	M	B	M	M

Fuente: Pasante del Proyecto

4 DIAGNOSTICO FINAL.

De la evaluación de los hallazgos, en la auditoría realizada de la evaluación a la seguridad física, lógica, infraestructura de red, servicio de mantenimiento de equipo y base de datos de la CLÍNICA SAN JOSÉ S.A.S., se concluye lo siguiente:

Los procedimiento de copias de respaldo de la información que se genera diariamente en la empresa no están siendo almacenados, ni protegidos de la mejor manera, lo que puede causar la pérdida total de la información y posiblemente las fallas en la red constantemente dañen el activo.

Se evidenció la falta de monitoreo preventivo al firewall, puesto que todas las operaciones basadas en la Red de datos son soportadas por el IPCop y cada procedimiento que se realiza en él debe estar sujeto al debido mantenimiento lógico y físico de este.

La Clínica carece de procedimientos formales y políticas para el debido manejo de los activos de información.

La Clínica carece de documentación de políticas, procedimientos, manuales o guías, que oriente los procesos y actividades que se realizan diariamente en las instalaciones.

Se evidencio un mal diseño e incumplimiento de normas de instalación de la red lo cual está causando la mala segmentación del tráfico de la red y poco a poco el deterioro del cableado de datos de la Clínica.

Poco monitoreo a los dispositivos como router, switch, Access Point, estabilizadores, y escasa adquisición de nuevos dispositivos de red que permitan el óptimo rendimiento de los mismos.

No existe ningún tipo de restricción al área de sistemas que impida la manipulación, el sabotaje de las herramientas de mantenimiento de cómputo.

No existen copias de la aplicación SIIS con sus respectivas mejoras, ni la documentación de las mismas.

5. CONCLUSIONES

La auditoría informática se encarga de gestionar y evaluar las vulnerabilidades que pudieran estar presentes en los sistemas de información. Una vez enfocada las inconsistencias de las empresas se documentan, se reportan los resultados a los gerentes o responsables de las instalaciones y se sugieren medidas que permitan mejorar la seguridad.

Al realizar el estudio del entorno a auditar, se pudo comprender y delimitar los alcances de todo este proceso, en donde se realizaron una serie de procedimientos y normas que permitieron de una manera eficiente y eficaz culminar este proyecto generando nuevas expectativas en cuanto a la seguridad de la información y el manejo que se le debe dar a las tecnologías de la informacion y la comunicación TIC.

En este proyecto se observó que el entorno informático de la Clínica San José S.A.S., presenta deficiencias en los aspectos relacionados con seguridad física y lógica de acuerdo con lo establecido en el estándar internacional ISO/IEC 27001 en el debido cumplimiento de las Normas de seguridad.

Se pudo evidenciar de igual manera que la Clínica carece de procedimientos formales y políticas para el debido manejo de los activos de información. Así mismo, no cuenta con la documentación de políticas, procedimientos, manuales o guías, que oriente los procesos y actividades que se realizan diariamente en las instalaciones. Este hecho genera un alto riesgo para la seguridad de los recursos informáticos de la Clínica objeto de auditoria.

6. RECOMENDACIONES

El uso de las tecnologías que utiliza la Clínica San José S.A.S objeto de estudio, como herramienta base en la administración de sus activos, ha influido a que la empresa requiera intervención de profesionales en el área informática con el fin de evaluar, identificar y controlar amenazas que puedan llegar a convertirse en riesgos para sus actividades y transacciones.

Basado en los resultados obtenidos en todo este proceso se recomienda lo siguiente:

Establecer y poner en práctica políticas sobre el resguardo de la informacion que se maneja a diario en la entidad.

Se recomienda que el jefe de sistemas solo tenga un único cargo dentro de la empresa, lo cual le facilitará estar al pendiente de todos los procedimientos que se realicen en el área.

Se sugiere la creación de un procedimiento para la continuidad de negocio tomando como base la ISO/IEC 27001.

Es de vital importancia documentar cada uno de los procedimientos que se lleven a cabo dentro de las instalaciones de la empresa.

Realizar un manual de funciones para los empleados del Área de Sistemas, lo cual permitirá medir el rendimiento de cada trabajador dependiendo de las funciones que se les sea asignada.

La Clínica San José S.A.S., debe establecer políticas que permita cumplir sus actividades con eficiencia, contribuyendo al desarrollo de las operaciones de la entidad y consecuente cumplimiento de los objetivos y metas que se planteen.

Se sugiere que se establezca e implementen políticas de seguridad de la información, donde se evidencie el compromiso y valor de los activos de la empresa.

La Clínica debe mejorar la forma como se lleva el programa de copias de seguridad e implementar las copias de respaldo automáticas o en la nube.

En caso que las copias de seguridad sigan siendo llevadas en Disco duros, se recomienda no tenerlas en el área de sistema, sino tener un sitio por fuera de las instalaciones donde estos discos duros no estén expuestos.

Realizar una reestructuración de la red de la empresa, donde se adquieran rack de comunicaciones en los cuales se puedan agrupar el switch y los router que están distribuidos por toda la clínica soportando los servicios de red.

Se recomienda realizar un constante monitoreo la Firewall, para proveer de una manera eficiente y eficaz cada servicio brindado por el mismo.

Implementar políticas para la adquisición de nuevos dispositivos de red, para optimizar los servicios de red.

Establecer restricciones para el ingreso de personal no autorizado al área de sistemas.

Implementar políticas para la documentación de todos los procesos que se realicen a nivel de software a la aplicación SIIS.

BIBLIOGRAFIA

CANO, Jeimy J., Computación Forense. Descubriendo los rastros informáticos, primera edición: Alfa omega Grupo Editor, México, Julio 2009.

DEL PESO NAVARRO, EMILIO; DEL PESO, MAR; PIATTINI VELTHUIS, MARIO G. (2008). Auditoría de Tecnologías y Sistemas de Información México: Alfa omega Ra-Ma.

Diseño de un sistema de gestión de SEGURIDAD DE INFORMACIÓN Óptica ISO 27001

ECHENIQUE GARCÍA, José Antonio, Auditoría en Informática, McGraw-Hill, México, 2001.

Estándar Internacional ISO 27001. Tecnología de la información – Técnicas de seguridad –Sistemas de gestión de seguridad de la información- Requerimiento

INTERNATIONAL ORGANIZATION FOR STANDARDIZATION. Information Technology. Security Techniques. Code of Practice for Information Security Management. Geneva: ISO/IEC, 2005, 107 P (ISOIIEC 27002:2005 (E)).

Universidad Carlos III de Madrid escuela politécnica superior calidad y seguridad de la información y auditoría Informática

VILAR BARRIO, José Francisco. La auditoría de los sistemas de gestión de la calidad, FC Editorial, 220 páginas, Agosto 1999

REFERENCIAS DOCUMENTALES ELECTRONICAS

Administración de los Riesgos en los Sistemas de Información. Administración de los riesgos en los sistemas de información como herramienta de gestión para los administradores.
<http://www.asfae.cl/Enefa_2002/Ponencia_8_extenso.pdf

Auditoría de Sistemas de Información. Seguridad informática: Conceptos básicos, Capítulo <http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/jerez_l_ca/capitulo1.pdf>

Auditoría Integral y seguridad de sistemas de informacion LTDA.
http://www.audisis.com/

Constitución política de Colombia. De la protección de la información y de los datos, Ley 1273 de 2009 <http://www.dmsjuridica.com/CODIGOS/LEGISLACION/LEYES/2009/LEY_1273_DE_2009.htm

Estándar ISO/IEC 27001
http://www.iso27001standard.com

FERNÁNDEZ, Eduardo. CFT soeduc concepto de auditoría <www.soeduc.cl/apuntes/concepto%20de%20auditoria.doc>
http://www.jkmst.com

Information Systems Audit And Control Association. Norma De Auditoría De SI, Ética Y Normas Profesionales Documento N° S3 Ética Y Estándares Profesionales. <http://www.isaca.org/Knowledge- Center/Standards/Documents/Standards-IT-Spanish-S3.pdf>

Integridad de los datos. El aspecto más relegado de la seguridad de la información http://www.isaca.org/Journal/Past-Issues/2011/Volume-6/Pages/Data-Integrity-Information-Securitys-Poor-Relation-spanish.aspx

Introducción a la auditoría de sistemas de información. Breve historia de la auditoría de sistemas de información.
<http://www.escet.urjc.es/~ai/T2Apuntes.pdf>

Sistema de gestión de seguridad de la información ISO/IEC 27001
http://www.tuv-sud.es/uploads/images/1350635458019372390409/pdf2-0039-iso-iec-27001-es-260412.pdf

Universidad Carlos III de Madrid escuela politécnica superior seguridad lógica y de accesos y su auditoría *proyecto fin de carrera* ingeniería técnica en informática de gestión

ANEXOS

Anexo A. Solicitud de Información inicial al Gerente de la Clínica

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

OF001

Barrancabermeja, Agosto 30 de 2013

Especialista
CRISTHIAN RODRÍGUEZ
Gerente General
Clínica San José S.A.S.
Ciudad

Asunto: Solicitud de documentos.

Cordial saludo.

Para dar inicio a las actividades contempladas en el Convenio Marco de Apoyo Interinstitucional para la realización de pasantías y/o prácticas profesionales, celebrado entre la Universidad Francisco de Paula Santander y la Clínica San José S.A.S., con objeto de realizar una evaluación a la Seguridad Física y Lógica de la Infraestructura tecnológica de la Clínica en mención, respetuosamente me permito solicitar la siguiente documentación:

- Filosofía Institucional de la Empresa
- Organigrama de la Empresa
- Manual de funciones de los empleados del área de Sistemas
- Manual de procedimientos del área de Sistemas
- Planes de seguridad del área de Sistemas
- Planes de contingencias
- Procedimientos formales de realización de copias de respaldo
- Procedimientos formales de soporte a usuarios
- Programas de mantenimiento de equipos de cómputo

En espera de su colaboración,

Atentamente,

Henry Marulanda P.

HENRY MARULANDA PADILLA
Estudiante de Pasantía

Rdo. Cristhi — Sol R
30-08-13

Anexo B. Solicitud dirigida al Coordinador de Procesos para obtener información con respecto al área de sistemas.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

OF002

Barrancabermeja, Agosto 30 de 2013

Ingeniero
NICOLÁS DE LA TORRE
Coordinador de Procesos Sistemas
Clínica San José S.A.S.
Ciudad

Asunto: Solicitud de documentos.

Cordial saludo.

Para dar inicio a las actividades contempladas en el Convenio Marco de Apoyo Interinstitucional para la realización de pasantías y/o prácticas profesionales, celebrado entre la Universidad Francisco de Paula Santander y la Clínica San José S.A.S., con objeto de realizar una evaluación a la Seguridad Física y Lógica de la Infraestructura tecnológica de la Clínica en mención, respetuosamente me permito solicitar la siguiente documentación:

- Manual de usuario de las aplicaciones
- Políticas de seguridad de las aplicaciones
- Políticas de acceso a usuarios tanto a áreas como a aplicaciones
- Bitácoras de realización de copias de respaldo

En espera de su colaboración,

Atentamente,

Henry Marulanda P.
HENRY MARULANDA PADILLA
Estudiante de Pasantía

V.B 30-08-13

Anexo C. Entrega de Documentación origina por la Clínica

ISO 9001: 2008
ISO 14001: 2004
OHSAS 18001: 2007
BUREAU VERITAS Certification
Nº236764 / Nº236765 / Nº236766

ONAC
ACREDITADO ISO/IEC 17021:2006 15-CSG-007

CLINICA SAN JOSÉ S.A.S.

NIT.800.255.963-4

CE00531-13
Barrancabermeja, 08 de Octubre de 2013

Estudiante de Pasantia
HENRY MARULANDA PADILLA
UNIVERSIDAD FRANCISCO DE PAULA SANTANDER
Ocaña

ASUNTO: ENTREGA DE DOCUMENTOS

Cordial Saludo,

La presente es para comunicarle que debido a la solicitud de información que usted ha presentado a la empresa, únicamente se le pueden facilitar los siguientes documentos:

- Manual de usuarios de las aplicaciones
- Filosofía Institucional de la Empresa
- Organigrama de la Empresa
- Programas de mantenimientos a los equipos de cómputo
- Procedimientos formales de realización de copias de seguridad

Agradezco su atención,

Atentamente,

NICOLÁS DE LA TORRE
Coordinador de Procesos

CALLE 47 No 28-05- COMUTADOR 6214852-6214968 TELEFAX: 6201960 BARRANCABERMEJA
Correo: clinicasanjose@clinicasanjosebarrancabermeja.com

Anexo D. PLAN DE AUDITORIA

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

PLAN DE AUDITORIA

TEMA

Evaluación mediante el estándar ISO 27001 de la Seguridad Física y Lógica de la infraestructura tecnológica de la Clínica san José S.A.S de la ciudad de Barrancabermeja – Santander.

OBJETIVOS

General

Evaluar mediante el estándar ISO 27001 de la Seguridad Física y Lógica de la infraestructura tecnológica de la Clínica san José S.A.S de la ciudad de Barrancabermeja – Santander.

Específicos

- Realizar el estudio inicial del entorno a auditar mediante la solicitud de la documentación necesaria.

- Diseñar los instrumentos de recolección de información necesarios para llevar a cabo la evaluación de cada una de los aspectos de la actual auditoría.

- Recolectar toda la información necesaria en cuanto a la seguridad física y lógica de las instalaciones de la Clínica se refiere.

- Elaborar el Informe Final de auditoría con la evaluación realizada a cada uno de los aspectos y su respectivo Plan de Recomendaciones.

RECURSOS

Para dar cumplimiento a todas las actividades de auditoría, será necesario la utilización eficiente de las siguientes herramientas:

Suministros de Oficina

- Tintas
- Papelería
- Fotocopias

Recursos de Hardware

- Equipos de cómputo
- Cámaras digitales
- Impresoras
- Línea telefónica
- Modem
- Conexión a Internet

Recursos de Software

- Microsoft Office 2010
- IDEA CaseWare 9.1
- Adobe Photoshop CS6
- Corel Draw CS6
- Motor de base de datos PostgreSQL

TIEMPO ESTIMADO

El presente Proyecto se ejecutará en un período de 4 meses calendario académico, en un horario de 7: 00 am a 12:00 m y de 2:00 a 6:00 pm en la ciudad de Barrancabermeja Santander.

CRONOGRAMA DE ACTIVIDADES

PROGRAMA DE AUDITORÍA			
ENTIDAD: CLINICA SAN JOSE S.A.S Barrancabermeja - Santander Área: Sistemas **PT. No. PA001** Fecha: 12-09-2013			
FASE	**ACTIVIDADES**	**TIEMPO ESTIMADO**	**RESPONS.**
I VISITA PRELIMINAR	▪ Definición del alcance y objeto de la auditoría. ▪ Visita a las instalaciones de la empresa. ▪ Solicitud de Documentación para el conocimiento de la organización. ▪ Solicitud de documentación del área a auditar. ▪ Solicitud de documentación de la aplicación objeto de auditoría.	UNA SEMANA	H.M.P.
II DISEÑO DE INSTRUMENTOS	▪ Elaboración de los cuestionarios. ▪ Diseño de entrevistas. ▪ Elaboración de formatos para observación. ▪ Elaboración de formatos para toma de evidencias (fotografías, vídeos, etc.).	CUATRO SEMANAS	H.M.P.
III EJECUCIÓN DE ACTIVIDADES	▪ Entrevistas a usuarios más relevantes de la dirección. ▪ Análisis de las claves de acceso, control, seguridad, confiabilidad y respaldos. ▪ Evaluación de los sistemas: Hardware y Software, evaluación del diseño lógico y del desarrollo del sistema. ▪ Evaluación del Proceso de Datos y de los Equipos de Cómputo: seguridad lógica, control de operación, seguridad física y procedimientos de respaldo.	TRES SEMANAS	H.M.P.
IV REVISION Y PRE-INFORME	▪ Revisión de los papeles de trabajo. ▪ Tabulación de instrumentos de recolección de datos. ▪ Determinación del Diagnóstico. ▪ Elaboración del Borrador.	UNA SEMANA	H.M.P. M.R.S.R.

V ELABORCIÓN DEL INFORME	▪ Elaboración del Informe técnico ▪ Elaboración del Informe Gerencial ▪ Presentación de los Informes	UNA SEMANA	H.M.P. M.R.S.R.

PA01: Programa de Auditoría H.M.P.: Henry Marulanda Padilla M.R.S.R.: Magreth Rossio Sanguino Reyes – Director Proyecto
APROBADO: Original Firmado Gerente General

PROCEDIMIENTOS DE AUDITORIA

Para hacer el proceso de recolección de información y de verificación de los resultados, con el fin de obtener las evidencias necesarias para soportar el Informe Final de Auditoría, se llevarán a cabo los siguientes procedimientos.

1. ENTREVISTAS

- Entrevista Inicial al Gerente, con el propósito de determinar el objeto y los límites de la Auditoría.

- Entrevista al Coordinador de Procesos, con el fin de evaluar la Seguridad Lógica de las aplicaciones de software de la Clínica San José.

- Entrevista al Coordinador de Procesos con el propósito de Evaluar los mecanismos de Seguridad Física en el ámbito informático de la Clínica San José S.A.S.

- Entrevista al Coordinador de Procesos para realizar la evaluación del servicio de mantenimiento de equipos de la Clínica San José S.A.S.

- Entrevista al Jefe de Mantenimiento para determinar la eficiencia de la prestación del servicio en cada uno de los equipos de cómputo que soportan las funciones de la Clínica.

- Entrevista al Administrador de Base de Datos, para determinar la integridad, confidencialidad y disponibilidad de la información contenida en la base de datos de la Clínica San José S.A.S.

2. CHECKLIST O LISTAS DE CHEQUEO

- Checklist de Rango para evaluar los evaluar los mecanismos de Seguridad Física en el ámbito informático de la Clínica San José S.A.S.

- Checklist Binario para evaluar los recursos de la Infraestructura de la Red de Datos de La Clínica San José S.A.S

- Checklist de Rango para la evaluación del servicio de Mantenimiento de Equipos de la Clínica San José S.A.S.

- Checklist de Rango para evaluar la Seguridad Lógica de las aplicaciones de software de la Clínica San José S.A.S.

- Checklist de Rango para evaluar la Seguridad Física de la Clínica San José S.A.S, en lo relacionado con aspectos técnicos de energía eléctrica, refrigeración y contingencias ante desastres.

3. FORMATOS DE VERIFICACIÓN

- Formato de verificación de los mecanismos de Seguridad Física.

- Formato de verificación de la Seguridad Lógica de las aplicaciones.

- Formato de evaluación de las tablas maestras de la Base de Datos.

Anexo E. GUIAS DE AUDITORIA

GUIAS DE AUDITORIA CLÍNICA SAN JOSE S.A.S

GUIA DE AUDITORIA	
ENTIDAD: CLINICA SAN JOSE	**PT. No. GA01**
Área: Sistemas	
Elaboró: H.M.P.	**Fecha: 14-09-2013**
Revisó: M.R.S.R.	**Fecha: 15-09-2013**
FASE I: VISITRA PRELIMINAR	

OBJETIVOS:

1. Establecer el objeto y los alcances de la Auditoría.
2. Hacer un reconocimiento general del entorno a auditar.
3. Realizar el estudio inicial del entorno a auditar.

ÍTEM	ACTIVIDADES	INICIAL	R/PT
1.1	Aplicación de entrevista al Gerente para determinar el propósito de la auditoría y los límites de la misma.	H.M.P.	EN001
2.1	Visita a las instalaciones de la empresa para reconocer físicamente la ubicación de cada una de las áreas de la misma.		
3.1	Solicitud de documentación general de la empresa y específica del área de Sistemas.		OF001
3.2	Solicitud de documentación de las aplicaciones y demás planes y programas de sistemas		OF002

GA01: Guía de Auditor
H.M.P.: HENRY MARULANDA PADILLA - Auditor
M.R.S.R.:MAGRETH ROSSIO SANGUINO REYES – Director Proyecto
EN001: Entrevista de iniciación realizada al Gerente
OF001: Oficio Nº 1
OF002:Oficio Nº 2

GUIA DE AUDITORIA	
ENTIDAD: CLINICA SAN JOSE **Área: Sistemas**	**PT. No. GA01**
Elaboró: H.M.P. **Revisó: M.R.S.R.**	**Fecha: 14-09-2013** **Fecha: 15-09-2013**
FASE II: DISEÑO DE INSTRUMENTOS	
OBJETIVOS: 1. Diseñar instrumentos de recolección de información	

ÍTEM	ACTIVIDADES	INICIAL	R/PT
1.1	Elaboración de formatos de entrevistas para evaluar aspectos generales al jefe de sistemas		
1.2	Construcción de Checklist de rango para evaluar seguridad física	H.M.P.	
1.3	Construcción de Checklist binario para evaluar seguridad lógica		
1.4	Elaboración de formatos para verificación de seguridad física		
1.5	Elaboración de formatos para verificación de seguridad lógica		

GA01: Guía de Auditor
H.M.P.: HENRY MARULANDA PADILLA - Auditor
M.R.S.R.:MAGRETH ROSSIO SANGUINO REYES – Director Proyecto

GUIA DE AUDITORIA		
ENTIDAD: CLINICA SAN JOSE S.A.S.		**PT. No. GA03 - 1**
Área: Sistemas		
	Elaboró: H.M.P.	**Fecha: 14-09-2013**
	Revisó: M.R.S.R.	**Fecha: 15-09-2013**
FASE III: EJECUCIÓN DE ACTIVIDADES		

OBJETIVOS:

1. Evaluar la Seguridad Física.
2. Evaluar la red de datos.
3. Evaluar el servicio de mantenimiento de equipos de cómputo.

ÍTEM	ACTIVIDADES	INICIAL	R/PT
1.1	Evaluación del cumplimiento de las políticas, planes y procedimientos de seguridad de los equipos e instalaciones.	H.M.P	
1.2	Evaluación de los controles de Seguridad Física teniendo en cuenta aspectos como: ▪ Controles de acceso a áreas críticas, ▪ Perímetros de seguridad. ▪ Cableado eléctrico y de datos. ▪ Suministro de energía eléctrica. ▪ Dispositivos para el control de incendios.		
2.1	Evaluación de la infraestructura de la red de datos y dispositivos de comunicación.		
3.1	Evaluación del servicio de mantenimiento de equipos y soporte técnico a usuarios.		

GA03 - 1: Guía de Auditoría Fase III página 1.
H.M.P.: HENRY MARULANDA PADILLA - Auditor
M.R.S.R.:MAGRETH ROSSIO SANGUINO REYES – Director Proyecto

GUIA DE AUDITORIA		
ENTIDAD: CLINICA SAN JOSE S.A.S.		**PT. No. GA03 - 2**
Área: Sistemas		
	Elaboró: H.M.P.	**Fecha: 14-09-2013**
	Revisó: M.R.S.R.	**Fecha: 15-09-2013**
FASE III: EJECUCIÓN DE ACTIVIDADES		
OBJETIVOS: 5. Evaluar la Seguridad Lógica.		

ÍTEM	ACTIVIDADES	INICIAL	R/PT
5.1	Evaluación de las herramientas de gestión de la seguridad de la información.	H.M.P.	
5.2	Verificación de las herramientas técnicas de protección de la información como: ▪ Control de acceso a las aplicaciones. ▪ Manejo de privilegios a usuarios. ▪ Software antivirus actualizado. ▪ Software antispyware. ▪ Firewall activo ▪ Entre otros.		
5.3	Verificación de la existencia y cumplimiento de las políticas de realización de copias de respaldo de la información crítica.		
5.40	Realización de pruebas a la base de datos para determinar su rendimiento.		

GA03 - 2: Guía de Auditoría Fase III página 2.
H.M.P.: HENRY MARULANDA PADILLA - Auditor
M.R.S.R.:MAGRETH ROSSIO SANGUINO REYES – Director Proyecto

GUIA DE AUDITORIA		
ENTIDAD: CLINICA SAN JOSE **Área: Sistemas**		**PT. No. GA01**
	Elaboró: H.M.P. **Revisó: M.R.S.R.**	**Fecha: 14-09-2013** **Fecha: 15-09-2013**
FASE IV: REVISION Y PRE-INFORME		

OBJETIVOS:

1. Diseñar un borrador del Informe final
2. Realizar un análisis profundo de la información obtenida

ÍTEM	ACTIVIDADES	INICIAL	R/PT
1.1	Organización de los papeles de trabajo.		
1.2	Procesamiento de los datos obtenidos durante el proceso		
2.1	Análisis de la información obtenida en el proceso	H.M.P	

GA01: Guía de Auditor
H.M.P.: HENRY MARULANDA PADILLA - Auditor
M.R.S.R.:MAGRETH ROSSIO SANGUINO REYES – Director Proyecto

GUIA DE AUDITORIA

ENTIDAD: CLINICA SAN JOSE **PT. No. GA01**

Área: Sistemas

Elaboró: H.M.P. **Fecha: 14-09-2013**

Revisó: M.R.S.R. **Fecha: 15-09-2013**

FASE V: ELABORCIÓN DEL INFORME

OBJETIVOS:

1. Elaborar el Informe Técnico
2. Elaborar el informe Gerencial
3. Presentar los Informes

ÍTEM	ACTIVIDADES	INICIAL	R/PT
1.1	Elaboración del Informe técnico para el área de sistemas		
2.1	Elaboración del informe Gerencial	H.M.P	
3.1	Presentación de Informes		

GA01: Guía de Auditor
H.M.P.: HENRY MARULANDA PADILLA - Auditor
M.R.S.R.:MAGRETH ROSSIO SANGUINO REYES – Director Proyecto

Anexo F. Entrevista Inicial al Gerente de la Clínica San José S.A.S.

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

EN001

Objetivo: Determinar el propósito y los límites de la Auditoría.

Entrevistado: **CRISTHIAN RODRÍGUEZ**

Cargo: **GERENTE GENERAL**

1) ¿A qué se dedica la clínica san José S.A.S de Barrancabermeja Santander?

Prestación de Servicios de Salud de 1er, 2do nivel de atención.

2) ¿Cuál es el tipo de población que la clínica san José atiende?

Población contributiva (EPS), población regimen Subsidiado (ARS), Especial (Ecopetrol, Magisterio), Accidentes de transito (SOAD), particular.

3) ¿Qué tiempo tiene usted de estar posesionado como gerente de la empresa?

2 Meses exactamente.

4) ¿Tiene usted conocimiento si alguna vez se ha llevado a cabo una auditoria a nivel informático en la empresa? Sí X No_____ ¿Cuáles fueron los resultados?

Optimización, Estructuración de Red y Ajuste del Sistema Integral de Información en Salud (SIIS) a las necesidades de la clínica San José.

5) ¿Cree usted conveniente realizar una auditoría a nivel informático en la empresa? ¿Por qué?

Optimización Estructura de Red y Ajuste del Sistema integral de información en salud (SIIS) a las necesidades de la Clinica San Jose.

6) ¿Cuáles son los motivos por los cuales usted desea que se realice una auditoría informática en la clínica san José de Barrancabermeja Santander?

Claro, Siempre es importante Saber las falencias, necesidades y Virtudes que posee la empresa y estar dispuesto a mejorar.

7) ¿Teniendo en cuenta la necesidad de realizar una Auditoria informática, que áreas específicas desea sean evaluadas?

Seguridad fisica y logica de la infraestructura tecnologica de la empresa.

Cristhian Sol R
ENTREVISTADO

Henry Parulanda P.
ENTREVISTADOR

Anexo G. Entrevista al Coordinador de Procesos para evaluar seguridad Física

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

EN003

Objetivo: Evaluar los elementos de seguridad física en el ámbito informático de la Clínica San José S.A.S.

Entrevistado: Ing. Nicolás De La Torre

Cargo: **Coordinador de Procesos**

1) ¿Qué mecanismo utiliza/implementa la empresa para la protección física de los equipos de cómputo?

UPS, Mantenimientos a los mismos y revisión del area.

2) ¿Cómo se lleva a cabo en la Clínica San José S.A.S la labor de Mantenimientos preventivos y correctivos a los equipos de cómputo?

Cada 6 meses Se realizan mantenimientos preventivos a los equipos de computo.

3) ¿Con que frecuencia?

Cada 6 meses

4) ¿De qué manera el responsable del mantenimiento entrega reportes de las tareas ejecutadas?

No se realizan informes de los mismos.

5) ¿Cómo se lleva a cabo el plan de mantenimiento preventivo de equipos contemplado dentro de las políticas de la empresa? Si existe claro está?

No existe tal política

6) ¿De qué manera se llevan a cabo las prohibiciones formales para el consumo de alimentos o bebidas cerca de los equipos de cómputo al igual que prohibiciones para fumar?

No se lleva a cabo tal procedimiento actualmente

7) ¿En caso de presentarse algún incendio, la Clínica San José S.A.S cuenta con algún mecanismo de alerta y de extinción de fuego?

Mecanismos de alerta no, pero existen extinto
y estos estan actualizados.

8) ¿Dónde está el inventario físico de los equipos de cómputo y dispositivos de comunicación que conforman la red de datos de la clínica San José?

Se lleva de manera digital y se encuentra en el area de Sistemas.

9) ¿Cuenta la clínica San José S.A.S con un circuito cerrado de televisión las 24 horas del día?

Actualmente no.

10) ¿Qué mecanismo de vigilancia interna existe en la Clínica?

Un vigilante de 10:00pm a 6:00 am certificado por una entidad (contrato E.V), y dos vigilantes contratados por la empresa en cuestión.

11) ¿Qué mecanismo de vigilancia externa existe en la Clínica?

No existe dicho mecanismo.

12) ¿Qué tipo de restricciones existen para el ingreso al área de sistemas?

No existe ningún tipo de restricción

13) ¿Qué mecanismo de identificación utiliza la Clínica para sus empleados en el momento de ingresar a sus instalaciones?

No existe ningún mecanismo que controle el ingreso del personal a la empresa.

ENTREVISTADO
NICOLAS DE LA TORRE
Coordinador de Procesos

Henry Marulanda P.

ENTREVISTADOR
HENRY MARULANDA PADILLA
Estudiante Pasantía

Anexo G1. Formato Checklist de Rango Seguridad Física

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

CHECKLIST DE RANGO

ENTIDAD: CLINICA SAN JOSE S.A.S. **PT. No. LV001**

Área: Seguridad Física

Elaboró: H.M.P. **Fecha: 16-09-2013**
Revisó: M.R.S.R. **Fecha: 18-09-2013**
Aplicó: H.M.P. **Fecha: 23-09-2013**

Aplicado a: Ing. Nicolás De La Torre – Coordinador de Procesos
Objetivo: Evaluar los elementos de seguridad física en el ámbito informático de la Clínica San José.

ÍTEM	PREGUNTA	E	B	R	I	R/PT
1.	¿Qué mecanismo utiliza/implementa la empresa para la protección física de los equipos de cómputo?	X				
2.	¿Cómo se lleva a cabo en la Clínica San José S.A.S la labor de Mantenimientos preventivos y correctivos a los equipos de cómputo?		X			
3.	¿Con que frecuencia?		X			
4.	¿De qué manera el responsable del mantenimiento entrega reportes de las tareas ejecutadas?				X	
5.	¿Cómo se lleva a cabo el plan de mantenimiento preventivo de equipos contemplado dentro de las políticas de la empresa? Si existe claro está.			X		
6.	¿De qué manera se llevan a cabo las prohibiciones formales para el consumo de alimentos o bebidas cerca de los equipos de cómputo al igual que prohibiciones para fumar?				X	
7.	¿En caso de presentarse algún incendio, la Clínica San José S.A.S cuenta con algún mecanismo de alerta y de extinción de fuego?		X			EF031
8.	¿Dónde está el inventario físico de los equipos de cómputo y dispositivos de comunicación que conforman la	X				IE001

	red de datos de la clínica San José?					
9.	¿Cuenta la clínica San José S.A.S con un circuito cerrado de televisión las 24 horas del día?				**X**	
10.	¿Qué mecanismo de vigilancia interna existe en la Clínica?			**X**		
11.	¿Qué mecanismo de vigilancia externa existe en la Clínica?				**X**	
12.	¿Qué tipo de restricciones existen para el ingreso al área de sistemas?				**X**	
13.	¿Qué mecanismo de identificación utiliza la Clínica para sus empleados en el momento de ingresar a sus instalaciones?				**X**	

H.M.P.: Henry Marulanda Padilla - Estudiante de Pasantía
M.R.S.R.: Magreth Rossio Sanguino Reyes – Director Proyecto
LV001: Checklist de Rango No. 1
E.: Excelente = 4
B.: Bueno = 3
R.: Regular= 2
I.: Insuficiente= 1
R/PT: Referenciación de los Papeles de trabajo
IE001: Inventario de equipos de cómputo
EF031: Evidencias Fotográficas

Después de aplicar el procedimiento de evaluación del Checklist para la seguridad física de las aplicaciones, se obtuvo el siguiente resultado.

Cantidad de Ítem = 13

Ítem 1= 4	Ítem 6= 1	Ítem 11= 1
Ítem 2 = 3	Ítem 7 = 3	Ítem 12= 1
Ítem 3 = 3	Ítem 8 = 4	Ítem 13 = 1
Ítem 4 = 1	Ítem 9 = 1	
Ítem 5 = 2	Ítem 10 = 2	

Subtotal = Σ **Ítem 1 hasta Ítem 13**
Subtotal = 27
Total = Subtotal / Cantidad de ítems
Total = 27 / 13
Total = 2.077 ≈ 2.1

Por lo anteriormente descrito en la fórmula, se puede concluir que La Seguridad Física en el ámbito informático de la Clínica San José S.A.S., es **Regular**, pues carece de políticas formales que permitan implementar medidas de protección para los recursos informáticos de la entidad.

Evaluado por

HENRY MARULANDA PADILLA
Estudiante de Pasantía

Revisado por

Ing. MAGRETH ROSSIO SANGUINO REYES
Director Proyecto

Evidencias para el Formato Checklist de Rango Seguridad Física PT. No. LV001

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

EXTINTORES CLINICA SAN JOSE S.A.S

PT. No. EF031

Foto 1. Extintor Cuarto Piso.

Foto 2. Extintor Tercer Piso.

Foto 3. Extintor Segundo Piso.

Foto 4. Extintor 1. Primer Piso.

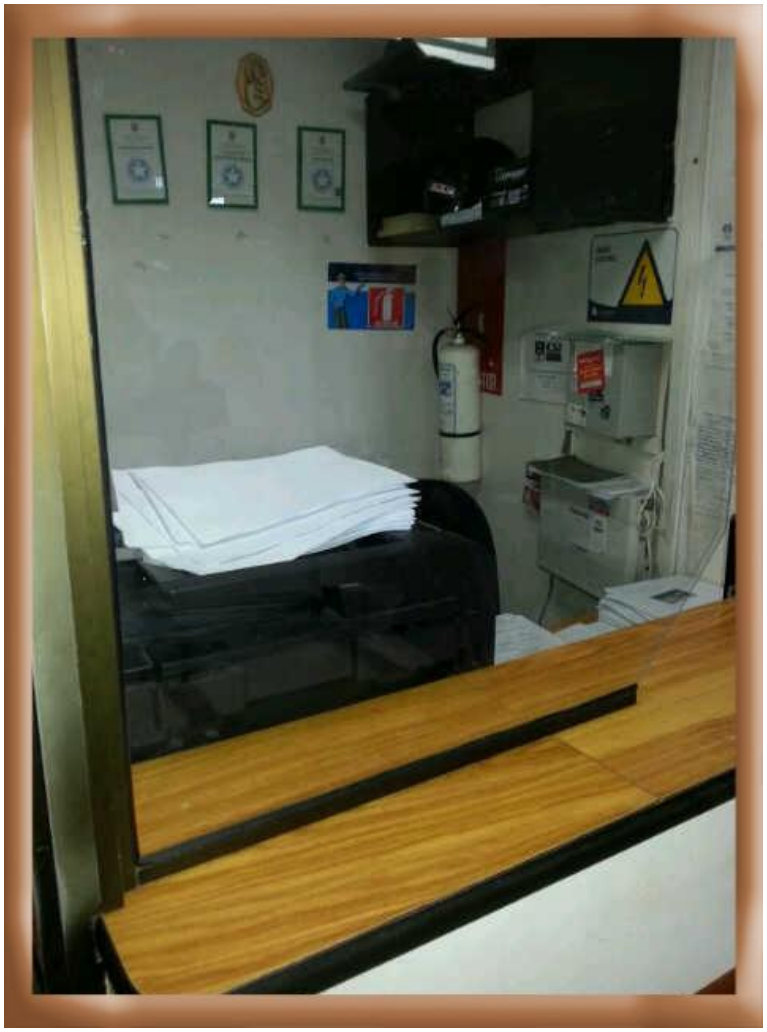


Foto 5. Extintor 2. Primer Piso.

Foto 6. Extintor 3. Primer Piso.

Foto 7. Extintor Sótano

CLINICA SAN JOSE S.A.S

INVENTARIO DE SISTEMAS

PT No. IE001

DEPARTAMENTO: Centro Ambulatorio

N. INVENTARIO	DESCRIPCION	REFERENCIA	MARCA	AREA
2273	Teclado	Kb-0316	HP	Recep Cent Ambulatorio
2275	CPU	Xl808av#219	HP	Recep Cent Ambulatorio
2276	Monitor	Hplv1911	HP	Recep Cent Ambulatorio
2277	Mouse	M-s0005-0	HP	Recep Cent Ambulatorio
1748	Impresora	Photo smart c4280	HP	Recep Cent Ambulatorio
1599	Teclado	K639	GENIUS	Fact Cent Ambulatirio
126	CPU	Clon	CLON	Fact Cent Ambulatirio
93	Monitor	Hsg 1044	QBEX	Fact Cent Ambulatirio
2279	Mouse	Xscroll	GENIUS	Fact Cent Ambulatirio
1340	Impresora	Laserjet P2055dn	HP	Fact Cent Ambulatirio
2278	Scaner	scanjet professional 1000	HP	Fact Cent Ambulatirio
2519	Teclado	BAUVTOBHH1A0NL	HP	Vacunacion
105	CPU	Kronos 5810290	QBEX	Vacunacion
104	Monitor	Hsg 1044	QBEX	Vacunacion
2282	Mouse	1f3f72d	QBEX	Vacunacion
782	Teclado	K9852	Delux	Consultorio 2
2283	CPU	Kronos 5810290	QBEX	Consultorio 2
89	Monitor	Hsg 1044	QBEX	Consultorio 2
115	Mouse	1f3f72d	QBEX	Consultorio 2
119	Teclado	KB-1000	OMEGA	Consultorio 3
109	CPU	Kronos 5810290	QBEX	Consultorio 3
117	Monitor	Hsg 1044	QBEX	Consultorio 3

2280	Mouse	Net scroll 120	GENIUS	Consultorio 3
1788	Teclado	Kb-06xe	QBEX	Fisioterapia
145	CPU	CLON	CLON	Fisioterapia
445	Monitor	T71w	BENQ	Fisioterapia
2281	Mouse	Gm-03022p	GENIUS	Fisioterapia
DEPARTAMENTO: Mantenimiento				
2284	Teclado	K639	GENIUS	Mantenimiento
2237	CPU	CLON	CLON	Mantenimiento
103	Monitor	Hsg 1044	QBEX	Mantenimiento
2285	Mouse	Net scroll 120	GENIUS	Mantenimiento
DEPARTAMENTO: Cuarto Piso UCI				
2138	Teclado	Kb-0316	HP	Equipo 1
2137	CPU	MXL2181JRP	HP	Equipo 1
2136	Monitor	LV1911	HP	Equipo 1
2139	Mouse	S-0005O	HP	Equipo 1
2142	Teclado	KB-0316	HP	Equipo 2
2141	CPU	MXL2180C27	HP	Equipo 2
2140	Monitor	LV1911	HP	Equipo 2
2143	Mouse	60053-002	HP	Equipo 2
DEPARTAMENTO: Tercer Piso				
2286	Teclado	KB-06XE	GENIUS	Enfermeria Equipo 1
1306	CPU	CLON	CLON	Enfermeria Equipo 1
2172	Monitor	T71W	DENQ	Enfermeria Equipo 1
2287	Mouse	Gm-03022p	GENIUS	Enfermeria Equipo 1
2175	Teclado	KB-0316	HP	Enfermeria Equipo 2
2288	CPU	COMPAQ 400 PRO SFF	HP	Enfermeria Equipo 2
2289	Monitor	LV1911	HP	Enfermeria Equipo 2
2176	Mouse	600553-002	HP	Enfermeria Equipo 2
1412	IMPRESORA	Laserjet P2055dn	HP	Enfermeria Equipo 2
2587	Teclado	Kb-110x	GENIUS	Facturacion
2198	CPU	Kronos 5810290	QBEX	Facturacion
2290	Monitor	Hsg 1044	QBEX	Facturacion

1016	Mouse	537750-001	GENIUS	Facturacion
DEPARTAMENTO: Segundo Piso				
1472	Teclado	KB-1000	OMEGA	Fact Cirugia
446	CPU	CLON	CLON	Fact Cirugia
2291	Monitor	Hsg 1044	QBEX	Fact Cirugia
1854	Mouse		Next	Fact Cirugia
2292	Impresora	F7bf031569	EPSON	Fact Cirugia
1474	Impresora	Laserjet P2055dn	HP	Fact Cirugia
128	Teclado	KB-1000	OMEGA	Enfermeros
2293	CPU	CLON	CLON	Enfermeros
118	Monitor	Hsg 1044	QBEX	Enfermeros
2485	Mouse	JW-cskm02	JAWAN	Enfermeros
1074	Computador Portatil	Presario C700	COMPAQ	Cirugia
2294	Computador Portatil	Aspire 4739	.ACER	Cirugia
2295	Teclado	K639	GENIUS	Cirugia
1335	CPU	Blue Code	CLON	Cirugia
1533	Monitor	W1943SG-PF	LG	Cirugia
2225	Mouse	216125e	QBEX	Cirugia
DEPARTAMENTO: Primer Piso				
2236	Teclado	KU-0138	GENIUS	Fact Urgencias
1172	CPU	5050MT	COMPAQ	Fact Urgencias
1171	Monitor	HP Le1901W	HP	Fact Urgencias
1174	Mouse	537750-001	GENIUS	Fact Urgencias
2296	Impresora	Lase Jet pro 400 MPF	HP	Fact Urgencias
2298	Teclado	K639	GENIUS	Consultorio 1
2300	CPU	TWIN 36102901	QBEX	Consultorio 1
2297	Monitor	IH182APB	QBEX	Consultorio 1
2299	Mouse	GM-03022P	GENIUS	Consultorio 1
2301	Teclado	SK-8115	DELL	Consultorio 2
2303	CPU	KRONOS 5810290	QBEX	Consultorio 2
125	Monitor	T71W	BENQ	Consultorio 2
2302	Mouse	GM-03022P	GENIUS	Consultorio 2
2304	Estabilizador	IEN-AVER1006	NEW	Consultorio 2

2307	Teclado	K639	GENIUS	Triage
890	CPU	KRONOS 5810290	QBEX	Triage
2306	Monitor	IH182APB	QBEX	Triage
2305	Mouse	Net scroll 120	GENIUS	Triage
2106	Computador Portatil	3c275176w	TOSHIBA	Triage
1921	Teclado	Sk-8110	DELL	Estcn enfermeria Eq1
2310	CPU	KRONOS 5810290	QBEX	Estcn enfermeria Eq1
55	Monitor	IH182APB	QBEX	Estcn enfermeria Eq1
2309	Mouse	GM-03022P	GENIUS	Estcn enfermeria Eq1
2308	Impresora	Hp Laser Jet P2035n	HP	Estcn enfermeria Eq1
2311	Estabilizador	Propc	NIOMAR	Estcn enfermeria Eq1
2314	Teclado	K639	GENIUS	Estcn enfermeria Eq2
97	CPU	KRONOS 5810290	QBEX	Estcn enfermeria Eq2
2312	Monitor	Hsg 1044	QBEX	Estcn enfermeria Eq2
2313	Mouse	GM-03022P	GENIUS	Estcn enfermeria Eq2
1772	Teclado	K639	GENIUS	Rayos X
435	CPU	CLON	CLON	Rayos X
1117	Monitor	W1934SI	LG	Rayos X
2315	Mouse	GM-03022P	GENIUS	Rayos X
2316	Impresora	GK420T	ZEBRA	Rayos X
DEPARTAMENTO: Farmacia				
2319	Teclado	539130-161	HP	Equipo 1
2317	CPU	MXL202020v	HP	Equipo 1

2318	Monitor	S1933	HP	Equipo 1
2320	Mouse	265966-011	HP	Equipo 1
2321	Teclado	Kb-0316	HP	Equipo 2
2323	CPU	MXL218146L	HP	Equipo 2
151	Monitor	913FW	AOC	Equipo 2
2566	Mouse	jw- cskm 02	JAWAN	Equipo 2
DEPARTAMENTO: Apoyo Diagnostico				
2324	Teclado	Kb-0316	HP	Apoyo Diagnostico
2327	CPU	MXL218146L	HP	Apoyo Diagnostico
2325	Monitor	Lv1911	HP	Apoyo Diagnostico
2326	Mouse	537748-001	HP	Apoyo Diagnostico
1349	Impresora	Laserjet P2055dn	HP	Apoyo Diagnostico
1904	Scaner	scanjet professional 1000	HP	Apoyo Diagnostico
DEPARTAMENTO: Laboratorio				
2328	Teclado	164.960.304.851	GENIUS	Laboratorio
422	CPU	CLON	DELUX	Laboratorio
779	Monitor	HW173A	QBEX	Laboratorio
1107	Mouse			Laboratorio
DEPARTAMENTO: Administracion				
2330	Teclado	Kb-0316	HP	Archivo
2332	CPU	MXL218146L	HP	Archivo
2331	Monitor	Lv1911	HP	Archivo
2329	Mouse	60053-002	HP	Archivo
2333	Estabilizador		NEW LINE	Archivo
2334	CPU	CLON	CLON	Secrt Auxiliar
434	Monitor	PL-19b	PROVIEW	Secrt Auxiliar
2336	Mouse	GM-03022P	GENIUS	Secrt Auxiliar
2337	Teclado	539130-161	HP	Fact. Y Auditoria
2340	CPU	MXL1151D18	HP	Fact. Y Auditoria
2339	Monitor	S2021	CONPAQ	Fact. Y Auditoria
2338	Mouse	26598-011	HP	Fact. Y Auditoria

2341	Teclado	K639	GENIUS	Glosas
1601	CPU	CLON	CLON	Glosas
1598	Monitor	E1920NX	SANSUNG	Glosas
2342	Mouse	60053-003	HP	Glosas
2343	Teclado	Kb-0316	HP	Auditoria Coomeva
2345	CPU	MXL1151D18	HP	Auditoria Coomeva
159	Monitor	716Sw	AOC	Auditoria Coomeva
2344	Mouse	Net scroll 120	GENIUS	Auditoria Coomeva
1305	Teclado	K639	GENIUS	Aux Administrativa
2402	CPU	CLON	CLON	Aux Administrativa
2347	Monitor	Lv1911	HP	Aux Administrativa
2346	Mouse	Net scroll 120	GENIUS	Aux Administrativa
2350	CPU	MXL202020G	HP	secretaria
2349	Monitor	LV1911	HP	secretaria
2348	Mouse	265966-011	HP	secretaria
1024	Teclado	KB-1000	OMEGA	secretaria
1359	Computador Portatil	ASPIRE 5338	.Acer	Jefe de Sistemas
2351	Mouse	Net scroll 100x	GENIUS	Jefe de Sistemas
2352	Teclado	539130-161	HP	Envíos
2354	CPU	MXL1151D00	HP	Envios
1631	Monitor	WM767A	COMPAQ	Envios
2353	Mouse	265966-011	HP	Envios
2356	Teclado	539130-161	HP	Director Administrativo
2357	CPU	MXL202020L	HP	Director Administrativo
2358	Monitor	XJ311A	HP	Director Administrativo
2355	Mouse	265966-011	HP	Director Administrativo

1173	Teclado	505130-011	HP	Gerente de Servicios
1634	CPU	MXL1011R6C	HP	Gerente de Servicios
1628	Monitor	S2021	COMPAQ	Gerente de Servicios
2359	Mouse	265986-011	HP	Gerente de Servicios
1629	Teclado	KB-1000	OMEGA	Salud Ocupacional 1
102	CPU	CLON	CLON	Salud Ocupacional 1
1212	Monitor	E170Sc	DELL	Salud Ocupacional 1
2360	Mouse	GM-03022P	GENIUS	Salud Ocupacional 1
2361	Estabilizador	Propc	NIOMAR	Salud Ocupacional 1
1301	Teclado	L-358c	QBEX	Salud Ocupacional 2
1211	CPU	CLON	CLON	Salud Ocupacional 2
2363	Monitor	E1942c-BN	LG	Salud Ocupacional 2
2362	Mouse	GM-03022P	GENIUS	Salud Ocupacional 2
2335	Teclado	53130-161X	HP	Aux Contable
2365	CPU	MXL1131BZ9	HP	Aux Contable
2366	Monitor	S2021	COMPAQ	Aux Contable
2364	Mouse	265986-011	HP	Aux Contable
2368	Teclado	KB-1000	OMEGA	Aux Tesoreria
2369	CPU	MXL2020217	HP	Aux Tesoreria
2370	Monitor	S1933	HP	Aux Tesoreria
2367	Mouse	265986-011	HP	Aux Tesoreria
2372	Teclado	CSS-720	PC SMART	Aux Cartera
2373	CPU		PC SMART	Aux Cartera
67	Monitor	HW173A	QBEX	Aux Cartera
2371	Mouse	CSS-720	PC SMART	Aux Cartera
2375	Teclado	K639	GENIUS	Contadora
149	CPU	CLON	CLON	Contadora
1308	Monitor	S19A300B	SANSUNG	Contadora
1663	Mouse	Net scroll 120	GENIUS	Contadora

2374	Impresora	LX-300+II	EPSON	Contadora
1720	Teclado	539130-161	HP	Gerencia
1723	CPU	MXL1611RSQ	HP	Gerencia
1719	Monitor	S2021	COMPAQ	Gerencia
1721	Mouse	265986-011	HP	Gerencia
DEPARTAMENTO: Avanzar				
415	Computador Portatil	ASPIRE 5338	.Acer	Odontologia Eqp 1
1317	Computador Portatil	ASPIRE 5338	.Acer	Odontologia Eqp 2
2376	Mouse	Xscroll	GENIUS	Odontologia Eqp 2
DEPARTAMENTO: Sistemas				
2221	Servidor	Power edge 2600	DELL	Sistemas
2222	Servidor	Power edge 2900	DELL	Sistemas
1030	Servidor	Power edge 2600	DELL	Sistemas
1046	Servidor	Power edge 1900	DELL	Sistemas
2223	UPS	Electra	QBEX	Sistemas
1013	UPS	Ecoserver ups	QUEST	Sistemas
2231	Rack	Super stack	3COM	Sistemas
2232	Dvr	tv-7216	Network dvr	Sistemas
76	Monitor	Hw 173a	QBEX	Sistemas
38	Monitor	Flatron ez t730sh	LG	Sistemas
1600	Mouse	Zmo 344	GENIUS	Sistemas
1075	Mouse	Um 2018	katec	Sistemas
87	Teclado	Y-UM76A	LOGITECH	Sistemas
144	Teclado	K639	GENIUS	Sistemas
1071	Radio	Pmn 4000d	MOTOROLA	Sistemas
1072	Radio	Pmn 4000d	MOTOROLA	Sistemas

Anexo H. Entrevista al jefe de mantenimiento para complementar factores ambientales

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

EN005

Objetivo: Evaluación a la Seguridad Física de la Clínica San José S.A.S

Entrevistado: **Ing. Leonardo Rojas**

Cargo: **Jefe de Mantenimiento**

1) ¿La red cuenta con un sistema de protección ante descargas eléctricas? ¿Cuál? , ¿Hace cuánto tiempo?, ¿Se ha modificado su estructura?

No Cuenta con este Sistema.

2) ¿La Clínica San José S.A.S posee algún plan de contingencia que permita el normal desempeño de las actividades, aun cuando se presente algún inconveniente? ¿Cómo se lleva a cabo este plan?

- Inundaciones
- Terremotos
- Corte en el flujo eléctrico
- Daño en los equipos

Fluido Electrico : Planta Electrica 60KBA

Inundaciones : Bomba Sumergible

3) ¿Existe conexión de polo a tierra para las instalaciones de los equipos de cómputo? ¿En qué lugar se encuentra?

Existe polo a Tierra Globalmente y Se encuentra en el Sotano. (Archivo Fotografico).

4) ¿Con que frecuencia se lleva a cabo del mantenimiento de los aires acondicionado de la Clínica San José S.A.S?

Mantenimiento Aires (Archivo Fotografico).

5) ¿El personal de mantenimiento está capacitado para el mejor desempeño de sus funciones? ¿Quién realiza tal capacitación, si existe claro está?

No Existen Capacitaciones.

6) ¿Cada cuanto se realizan estas capacitaciones?

NO Se realizan

ENTREVISTADO

Henry Marulanda

ENTREVISTADOR

Anexo H1. Formato Checklist de Rango Seguridad Física

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

CHECKLIST DE RANGO

ENTIDAD: CLINICA SAN JOSE S.A.S. **PT. No. LV005**
Área: Sistemas **Fecha: 16-09-2013**
Elaboró: H.M.P. **Fecha: 18-09-2013**
Revisó: M.R.S.R. **Fecha: 23-09-2013**

Aplicado a: Ing. Leonardo Rojas – Jefe de Mantenimiento
Objetivo: Evaluación a la Seguridad Física de la Clínica San José S.A.S

ÍTEM	PREGUNTA	E	B	R	I	R/PT
1.	¿La red cuenta con un sistema de protección ante descargas eléctricas? ¿Cuál? , ¿Hace cuánto tiempo?, ¿Se ha modificado su estructura?				X	
2.	¿La Clínica San José S.A.S posee algún plan de contingencia que permita el normal desempeño de las actividades, aun cuando se presente algún inconveniente? ¿Cómo se lleva a cabo este plan? ▪ Inundaciones ▪ Terremotos ▪ Corte en el flujo eléctrico ▪ Daño en los equipos		X			EF028
3.	¿Existe conexión de polo a tierra para las instalaciones de los equipos de cómputo? ¿En qué lugar se encuentra?	X				EF008
4.	¿Con que frecuencia se lleva a cabo del mantenimiento de los aires acondicionados de la Clínica San José S.A.S?	X				MA001
5.	¿El personal de mantenimiento está capacitado para el mejor desempeño de sus funciones? ¿Quién realiza tal capacitación, si existe claro está?				X	
6.	¿Cada cuánto se realizan estas capacitaciones?				X	

H.M.P.: Henry Marulanda Padilla
M.R.S.R.: Magreth Rossio Sanguino Reyes – Director Proyecto
LV005.: Checklist de Rango No. 5
R/PT: Referenciación de los Papeles de trabajo
E.: Excelente = 4
B.: Bueno = 3
R.: Regular = 2
I.: Insuficiente = 1
R/PT: Referenciación de los Papeles de trabajo
EF028-EF008: Evidencias Fotográficas
MA001: Mantenimientos de Aires

Después de aplicar el procedimiento de evaluación del Checklist para la seguridad física de las aplicaciones, se obtuvo el siguiente resultado.

Cantidad de Ítems = 6

Ítem 1= 1	Ítem 6= 1
Ítem 2 = 3	Ítem 4 = 4
Ítem 3 = 4	Ítem 5 = 1

Subtotal = Σ Item 1 hasta Item 5
Subtotal = 14
Total = Subtotal / Cantidad de ítems
Total = 14/ 6
Total = 2.3

De acuerdo con el estudio realizado a la seguridad física de la Clínica San José se puede inferir que el estado de la misma es **Regular**, puesto que aunque existen mecanismos de protección ante fallas eléctricas e inundaciones, no existe un plan de contingencia que permita dar continuidad a los servicios ofrecidos por la Clínica ante un evento inesperado.

Evaluado por

HENRY MARULANDA PADILLA
Estudiante de Pasantía

Revisado por

Ing. MAGRETH ROSSIO SANGUINO REYES
Director Proyecto

Evidencias para el Formato Checklist de Rango Seguridad Física PT. No. LV005

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

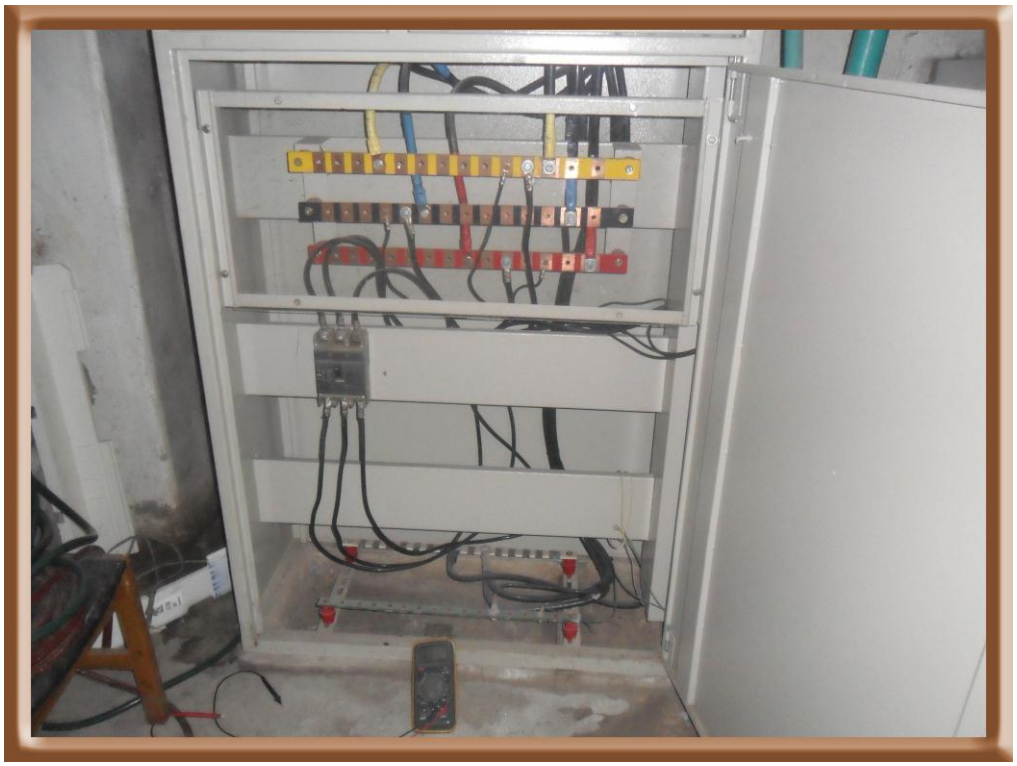
SEGURIDAD FÍSICA CLINICA SAN JOSE S.A.S

PT. No. EF028

Foto 1. Planta Eléctrica

Foto 2. Bomba Sumergible

Evidencia Fotográfica <u>EF008</u> para el Formato Checklist de Rango Seguridad Física



Evidencias para el Formato Checklist de Rango Seguridad Física PT. No. MA001

PT No. MA001

MANTENIMIENTO AIRES 2013

EQUIPOS	ENE	FEB	MAR	ABR	MAY	JUN	JUL	AGO	SEP	OCT	NOV	DIC
CHILLER 1	X			X			X			X		
CHILLER 2	X			X			X			X		
CHILLER 3		X			X			X			X	
CHILLER 4		X			X			X			X	
CHILLER 5			X			X			X			X
CHILLER 6			X			X			X			X
CHILLER 7			X			X			X			X
AIRES C.A.		X				X				X		
AVANZAR						X						X
COMPRAS	X			X			X			X		
RECEPCION PTO COOMEVA	X			X			X			X		
CONSULTORIO COOMEVA		X			X			X			X	
LABORATORIO	X			X			X			X		
PASILLO TOMA MUESTRA				X						X		
ADMINISTRACION	X						X					
GERENCIA					X						X	
IMAGENOLOGIA			X						X			
MANEJADORAS URGENCIAS			X			X			X			X
FANCOIL 2DO PISO		X	X									
FANCOIL 3R PISO		X	X									
FANCOIL OBSERVACIONES	X											
AIRES CIRUGIA		X			X			X			X	
AIRE RADIOLOGIA	X			X			X			X		
AIRES UCI		X			X			X			X	

NOTA: ESTAS FECHAS DE MANTENIMIENTO ESTAS DISPUESTAS A CAMBIOS.

LEONARDO ROJAS.

ANEXO I. Inventario de las Aplicaciones Instaladas a los equipos de cómputo

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

Evaluación de la seguridad lógica. La Clínica San José S.A.S., posee el siguiente inventario de software: existen 51 equipos de cómputo con las siguientes especificaciones:

Equipo No. 1: Facturación Centro Ambulatorio

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 1 GB
Capacidad del disco duro: 160 GB
Procesador: INTEL DUAL CORE 1.8 GHz

Cuadro 1. Equipo No. 1: Facturación Centro Ambulatorio

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Free
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Generador de Furisp	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 2: Recepción Centro Ambulatorio

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 2. Equipo No. 2: Recepción Centro Ambulatorio

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No.3: Vacunación

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 3. Equipo No. 3: Vacunación

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No.4: Consultorio 2

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 4. Equipo No. 4: Consultorio 2

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No.5: Consultorio 3

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 5. Equipo No. 5: Consultorio 3

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 6: Fisioterapia

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 1 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 1.8 GHz

Cuadro 6. Equipo No. 6: Fisioterapia

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 7: Mantenimiento

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 768 MB
Capacidad del disco duro: 160 GB
Procesador: Pentium 4 de 2.8 GHz

Cuadro 7. Equipo No. 7: Mantenimiento

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 8: UCI Equipo 1

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 8. Equipo No. 8: UCI Equipo 1

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 9: UCI Equipo 2

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 9. Equipo No. 9: UCI Equipo 2

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 10: Tercer Piso Equipo Enfermera Jefe 1

Sistema Operativo: Microsoft Windows 7 Ultímate Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 10. Equipo No. 10: Tercer Piso Equipo Enfermera Jefe 1

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 11: Tercer Piso Equipo 2

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 1 GB
Capacidad del disco duro: 1.50 GB
Procesador: INTEL DUAL CORE 1.6 GHz

Cuadro 11. Equipo No. 11: Tercer Piso Equipo 2

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 12: Tercer Piso Facturación

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 12. Equipo No. 12: Tercer Piso Facturación

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Generador de Furisp	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 13: Segundo Piso Facturación Cirugía

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 1 GB
Capacidad del disco duro: 160 GB
Procesador: Pentium 1.8 GHz

Cuadro 13. Equipo No. 13: Segundo Piso Facturación Cirugía

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet	Free
SIIS (Sistema integral de información en salud)	Licenciado
Generador de Furisp	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 14: Segundo Piso Enfermeros

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 512 MB
Capacidad del disco duro: 160 GB
Procesador: Pentium 1.8 GHz

Cuadro 14. Equipo No. 14: Segundo Piso Enfermeros

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 15: Segundo Piso Portátil 1 Cirugía

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 250GB
Procesador: INTEL DUAL CORE 2.2 GHz

Cuadro 15. Equipo No. 15: Segundo Piso Portátil 1 Cirugía

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 16: Segundo Piso Portátil 2 Cirugía

Sistema Operativo: Microsoft Windows 7 Ultimate Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 320 GB
Procesador: INTEL DUAL CORE 1.8 GHz

Cuadro 16. Equipo No. 16: Segundo Piso Portátil 2 Cirugía

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

.

Equipo No. 17: Segundo Piso Cirugía

Sistema Operativo: Red Hat Linux Ubuntu 10.04
Memoria RAM: 1 GB
Capacidad del disco duro: 160 GB
Procesador: INTEL DUAL CORE 2.2 GHz

Cuadro 17. Equipo No. 17: Segundo Piso Cirugía

Programas	**Licencia**
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Open Office	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 18: Primer Piso Facturación Urgencias

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 250 GB
Procesador: INTEL DUAL CORE 2.2 GHz

Cuadro 18. Equipo No. 18: Facturación Urgencias

Programas	**Licencia**
Microsoft Esencial	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Generador de Furisp	Licenciado
Ccleaner	Free
Base de datos Sivigila	Licenciado por la alcaldía

Fuente: Pasante del proyecto.

Equipo No. 19: Primer Piso Consultorio 1

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 19. Equipo No. 19: Primer Piso consultorio 1

Programas	**Licencia**
Microsoft Esencial	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 20: Primer Piso Consultorio 2

Sistema Operativo: Red Hat Linux Ubuntu
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 20. Equipo No. 20: Primer Piso consultorio 2

Programas	**Licencia**
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Open Office	Free
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 21: Primer Piso Triage

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 21. Equipo No. 21: Primer Piso Triage

Programas	**Licencia**
Microsoft Esencial	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 22: Primer Piso Triage Portátil

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 3 GB
Capacidad del disco duro: 500 GB
Procesador: Intel Pentium 2.7 GHz

Cuadro 22. Equipo No. 22: Primer Piso Triage Portátil

Programas	**Licencia**
Microsoft Esencial	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de información en salud)	Licenciado
Ccleaner	Free
Base de datos Sivigila	Licenciado de la alcaldia

Fuente: Pasante del proyecto.

Equipo No. 23: Primer Piso Estación enfermería Equipo 1

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 1 GB
Capacidad del disco duro: 160 GB
Procesador: Pentium 1.8 GHz

Cuadro 23. Equipo No. 23: Primer Piso Estación enfermería Equipo 1

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 24: Primer Piso Estación enfermería Equipo 2

Sistema Operativo: Red Hat Linux Ubuntu
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 24. Equipo No. 24: Primer Piso Estación enfermería Equipo 2

Programas	**Licencia**
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Open Office	Free
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 25: Primer Piso Rayos X

Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 1 GB
Capacidad del disco duro: 80 GB
Procesador: Pentium 1.6 GHz

Cuadro 25. Equipo No. 25: Primer Piso Rayos X

Programas	**Licencia**
Adobe Reader XI	Free
Winrrar	Licencia pre instalada
Microsoft Office 2010 Professional	Free
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free
Zefra	Free

Fuente: Pasante del proyecto.

Equipo No. 26: Farmacia Equipo 1

Sistema Operativo: Microsoft Windows 7 Ultímate Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 26. Equipo No. 26: Farmacia Equipo 1

Programas	**Licencia**
Microsoft Esencial	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 27: Farmacia Equipo 2

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 320 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 27. Equipo No. 27: Farmacia Equipo 2

Programas	**Licencia**
Microsoft Esencial	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 28: Apoyo Diagnostico

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 3.6 GHz

Cuadro 28. Equipo No. 28: Apoyo Diagnostico

Programas	**Licencia**
Microsoft Esencial	Free
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 29: Laboratorio

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 1 GB
Capacidad del disco duro: 160 GB
Procesador: INTEL DUAL CORE 1.8 GHz

Cuadro 29. Equipo No. 29: Laboratorio

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
Winrrar	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

.

Equipo No. 30: Administración Archivo

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.8 GHz

Cuadro 30. Equipo No. 30: Administración Archivo

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 31: Administración Secretaria Auxiliar

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 512 GB
Capacidad del disco duro: 80 GB
Procesador: INTEL DUAL CORE 2.1 GHz

Cuadro 31. Equipo No. 31: Administración Secretaria Auxiliar

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
Winrrar	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 32: Administración Facturación y Auditorias

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.9 GHz

Cuadro 32. Equipo No. 32: Administración Facturación y Auditorias

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
Winrrar	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 33: Administración Glosas

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.9 GHz

Cuadro 33. Equipo No. 33: Administración Glosas

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 34: Administración Auditoria Coomeva

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 3.9 GHz

Cuadro 34. Equipo No. 34: Administración Auditoria Coomeva

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
Winrrar	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo No. 35: Administración Auxiliar Administrativo

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 2 GB
Capacidad del disco duro: 160 GB
Procesador: INTEL DUAL CORE 2.2 GHz

Cuadro 35. Equipo No. 35: Administración Auxiliar Administrativo

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo 36. Administración Secretaria Gerencia

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.9 GHz

Cuadro 36. Equipo No. 36: Administración Secretaria Gerencia

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free
Paiper Pot	Version Free

Fuente: Pasante del proyecto.

Equipo 37. Administración Jefe de Sistemas

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 250 GB
Procesador: INTEL DUAL CORE 1.8 GHz

Cuadro 37. Equipo No. 37 Administración Jefe de Sistemas

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
Winrrar	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free
Putty	Free
WinSCP	Free
D-ViewCam	Free

Fuente: Pasante del proyecto.

Equipo 38. Administración Envíos

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.9 GHz

Cuadro 38. Equipo No. 38 Administración Envíos

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo 39. Administración Director Administrativo

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.9 GHz

Cuadro 39. Equipo No. 39: Administración Director Administrativo

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo 40. Administración Gerente de Servicios

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.9 GHz

Cuadro 40. Equipo No. 40: Administración Gerente de Servicios

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free
Sivigila	Licenciado por la Alcaldia

Fuente: Pasante del proyecto.

Equipo 41. Administración Salud Ocupacional 1

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 512GB
Capacidad del disco duro: 80 GB
Procesador: AMD ATHLON 1 GHz

Cuadro 41. Equipo No. 41: Administración Salud Ocupacional 1

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo 42. Administración Salud Ocupacional 2

Sistema Operativo: Microsoft Windows XP Profesional Versión 2002
Memoria RAM: 1 GB
Capacidad del disco duro: 160GB
Procesador: INTEL DUAL CORE 3.6 GHz

Cuadro 42 Equipo No. 42: Administración Salud Ocupacional 2

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
Winrrar	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo 43. Administración Auxiliar Contable

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.9 GHz

Cuadro 43. Equipo No. 43: Administración Auxiliar Contable

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo 44. Administración Auxiliar Tesorería

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.9 GHz

Cuadro 44. Equipo No. 44: Administración Auxiliar Tesorería

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Autor del proyecto.

Equipo 45. Administración Auxiliar Cartera

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.9 GHz

Cuadro 45. Equipo No. 45: Administración Auxiliar Cartera

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo 46. Administración Contadora

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.2 GHz

Cuadro 46. Equipo No. 46: Administración Contadora

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
Winrrar	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free
Programa JAL	Licenciado

Fuente: Pasante del proyecto.

Equipo 47. Administración Gerencia

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 500 GB
Procesador: INTEL DUAL CORE 2.9 GHz

Cuadro 47. Equipo No. 47: Administración Gerencia

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Free
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo 8 Avanzar Portátil 1

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 250 GB
Procesador: INTEL DUAL CORE 1.8 GHz

Cuadro 48. Equipo No. 48: Avanzar Portátil 1

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
Winrrar	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo 49. Avanzar Portátil 2

Sistema Operativo: Microsoft Windows 7 Profesional Versión 2009
Memoria RAM: 2 GB
Capacidad del disco duro: 250 GB
Procesador: INTEL DUAL CORE 1.8 GHz

Cuadro 49. Equipo No. 49: Avanzar Portátil 2

Programas	**Licencia**
Avast Antivirus	Licencia corporativa
Adobe Reader XI	Free
WinRAR	Licencia pre instalada
Microsoft Office 2010 Professional	Licenciado
Skype	Free
Nero	Free
Navegadores (Moxilla, google chrome, Internet explorer)	Free
SIIS (Sistema integral de informacion en salud)	Licenciado
Ccleaner	Free

Fuente: Pasante del proyecto.

Equipo 50. Sistemas Servidor Power edge 2600

Sistema Operativo: Red Hat Linux Ubuntu 10.04
Memoria RAM: 4 GB
Capacidad del disco duro: 160 GB
Procesador: INTEL DUAL CORE 2.2 GHz

Programas	Licencia
IPCop	Red Had Linux

Fuente: Pasante del proyecto.

Equipo 51. Sistemas Servidor Power edge 2900

Sistema Operativo: Red Hat Linux CentOs 4.8
Memoria RAM: 8 GB
Capacidad del disco duro: 250 GB
Procesador: INTEL DUAL CORE 2.2 GHz

Programas	Licencia
Sistema Integral de información en salud SIIS	Red Had Linux

Fuente: Pasante del proyecto.

Anexo J. Entrevista al Coordinador de Procesos para evaluar Seguridad Lógica

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

EN002

Objetivo: Evaluación de la Seguridad Lógica de la Clínica San José S.A.S

Entrevistado: Ing. Nicolás De La Torre
Cargo: Coordinador de Procesos

1) ¿Qué tipo de control existe para acceder a los equipos de cómputo o a los programas de software?

Al equipo como tal se debe acceder por medio de una contraseña y de igual forma al (SIIS)

2) ¿Qué políticas posee la Clínica San José S.A.S para mantener la confidencialidad, integridad y disponibilidad de la información que se genera?

Política como tal no existe, pero dependiendo la información se tiene una persona encargada para velar por esa Seguridad, integridad y disponibilidad.

3) ¿Cómo se cumplen estas políticas?

Segun el cargo de la persona se le da acceso a cierta información, cumpliendo así con su etica profesional

4) ¿Cómo se registra el cumplimiento de estas políticas?

No se realiza este registro de cumplimiento, pero cada persona debe cumplir con sus funciones diarias.

5) ¿Qué mecanismos utiliza La Clínica para generar conciencia en sus empleados de la importancia de proteger la información que manejan?

No se lleva a cabo cierta actividad, no se utilizan mecanismos, esto se realiza de forma verbal, e informal.

6) ¿Qué tipo de mecanismo se utiliza para el ingreso a las aplicaciones?

Usuario y Contraseña y algunas carpetas en comparticla de solo lectura.

7) ¿Dónde se encuentran las copias de las claves de acceso de los usuarios?

En la Base de Datos (Servidor)

8) ¿Existen un acuerdo de confidencialidad entre la Clínica San José S.A.S y los empleados para la protección de la información que les ha sido encomendada? ¿Qué estable este acuerdo?

Formalmente no existe este acuerdo.

9) ¿Qué pasa con las claves de acceso de esas personas que han dejado de laborar en la empresa?

Se colocan en estado Inactivo

10) ¿Cómo se lleva a cabo la capacitación periódica a los usuarios en el adecuado manejo de los equipos y de los aplicativos?

Solo se capacita al ingresar a la empresa y solo al aplicativo mas no al manejo del P.C.

11) ¿Cómo hace la empresa para saber si estas capacitaciones fueron exitosas?

Se realiza un Seguimiento de esa persona nueva que ingresa a la empresa (Verbal)

12) ¿Cómo se realizan las copias de seguridad de la información que se genera al interior de la Clínica San José S.A.S?

Ver Anexo (Manual de manejo y diligenciamiento de historias clínicas).

13) ¿Dónde almacenan estas copias de respaldo (Caja fuerte, mueble con cerradura, otros)?

En un Disco Duro y Se guarda en la misma oficina de Sistemas.

14) ¿Qué medios utilizan para realizar las copias de la información (CD, DVD, MEMORIAS USB, DISCOS DUROS)?

Disco Duro.

15) ¿Qué tipo de programas utiliza el área de sistemas de la Clínica San José S.A.S para el proceso de recuperación de archivos en caso de falla?

Hirens Boot, Comando CHKDSK (Windows), Easy Recovery.

16) ¿Qué tipo de software utiliza el área de sistemas para la detección de intrusos?

Se realiza a traves del IPCop

17) ¿Qué software antivirus poseen los equipos de la Clínica San José S.A.S?

AVAST Antivirus, Microsoft Essential, Licencia de AVAST Coorporativa 35 equipos

18) ¿Cada cuánto se actualizan las bases de datos de estos antivirus?

Automaticamente.

19) ¿Cuáles son los procedimientos para evitar la ejecución de programas no autorizados?

Bloqueo en el Firewall y en el Proxy a traves del IPCop (corta fuego con Intrfaz web).

20) ¿Cómo se documentan los procedimientos realizados por el personal de sistemas?

No se documentan, no se llevan Bitácoras.

21) ¿Cómo se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento?

Puerta con candado.

ENTREVISTADO
NICOLAS DE LA TORRE
Coordinador de Procesos

Henry Marulanda P.

ENTREVISTADOR
HENRY MARULANDA PADILLA
Estudiante Pasantía

Anexo J1. Formato Checklist de Rango Seguridad Lógica

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

CHECKLIST RANGO

ENTIDAD: CLINICA SAN JOSE S.A.S. **PT. No. LV004**
Área: Seguridad Lógica

Elaboró: H.M.P. **Fecha: 16-09-2013**
Revisó: M.R.S.R. **Fecha: 18-09-2013**
Aplicó: H.M.P. **Fecha: 29-09-2013**

Aplicado a: Ing. Nicolás De La Torre – Coordinador de Procesos
Objetivo: Evaluación a la Seguridad Lógica de la Clínica San José S.A.S

ÍTEM	PREGUNTA	E	B	R	I	R/PT
1.	¿Qué tipo de control existe para acceder a los equipos de cómputo o a los programas de software?	X				EF032
2.	¿Qué políticas posee la Clínica San José S.A.S para mantener la confidencialidad, integridad y disponibilidad de la información que se genera?			X		
3.	¿Cómo se cumplen estas políticas?			X		
4.	¿Cómo se registra el cumplimiento de estas políticas?				X	
5.	¿Qué mecanismos utiliza La Clínica para generar conciencia en sus empleados de la importancia de proteger la información que manejan?				X	
6.	¿Qué tipo de mecanismo se utiliza para el ingreso a las aplicaciones?	X				EF033
7.	¿Dónde se encuentran las copias de las claves de acceso de los usuarios?	X				
8.	¿Existen un acuerdo de confidencialidad entre la Clínica San José S.A.S y los empleados para la protección de la información que les ha sido encomendada? ¿Qué estable este acuerdo?				X	
9.	¿Qué pasa con las claves de acceso de esas personas		X			

	que han dejado de laborar en la empresa?					
10.	¿Cómo se lleva a cabo la capacitación periódica a los usuarios en el adecuado manejo de los equipos y de los aplicativos?			X		
11.	¿Cómo hace la empresa para saber si estas capacitaciones fueron exitosas?		X			
12.	¿Cómo se realizan las copias de seguridad de la información que se genera al interior de la Clínica San José S.A.S?		X			
13.	¿Dónde almacenan estas copias de respaldo (Caja fuerte, mueble con cerradura, otros)?			X		
14.	¿Qué medios utilizan para realizar las copias de la información (CD, DVD, MEMORIAS USB, DISCOS DUROS)?		X			
15.	¿Qué tipo de programas utiliza el área de sistemas de la Clínica San José S.A.S para el proceso de recuperación de archivos en caso de falla?		X			
16.	¿Qué tipo de software utiliza el área de sistemas para la detección de intrusos?		X			**EF029**
17.	¿Qué software antivirus poseen los equipos de la Clínica San José S.A.S?	X				
18.	¿Cada cuánto se actualizan las bases de datos de estos antivirus?	X				
19.	¿Cuáles son los procedimientos para evitar la ejecución de programas no autorizados?	X				**EF030**
20.	¿Dónde se archivan las bitácoras del sistema del equipo de cómputo?				X	
21.	¿Cómo se restringe el acceso a los lugares asignados para guardar los dispositivos de almacenamiento?				X	

H.M.P.: Henry Marulanda Padilla – Estudiante Pasantía
M.R.S.R.: Magreth Rossio Sanguino Reyes – Director Proyecto
LV004.: Checklist de Rango No. 004
E.: Excelente = 4
B.: Bueno = 3
R.: Regular = 2
I.: Insuficiente = 1
R/PT: Referenciación de los Papeles de trabajo
EF029-EF030-EF032-EF033: Evidencias Fotográficas

Para evaluar la Seguridad Lógica de la Clínica San José, se utilizó el siguiente procedimiento:
Cantidad de Ítems = 21

Ítem 1 = 4	Ítem 8 = 1	Ítem 15 = 3
Ítem 2 = 2	Ítem 9 = 3	Ítem 16= 3
Ítem 3 = 2	Ítem 10 = 2	Ítem 17 = 4
Ítem 4 = 1	Ítem 11 = 3	Ítem 18 = 4
Ítem 5 = 1	Ítem 12= 3	Ítem 19= 4
Ítem 6 = 4	Ítem 13 = 2	Ítem 20 = 1
Ítem 7 = 4	Ítem 14 = 3	Ítem 21 = 1

Subtotal = Σ Item 1 hasta Item 21
Subtotal = 55
Total = Subtotal / Cantidad de ítems
Total = 55 / 21
Total = 2.62 ≈ 3 .0
De acuerdo con el resultado obtenido, se llegó a la conclusión que la Seguridad Lógica de la Clínica San José es **Buena**, puesto que cuentan con restricciones de acceso a la información crítica de la entidad, pero es inadecuada y de alto riesgo, la manera en que resguardan las copias de respaldo de dicha información.

Evaluado por

HENRY MARULANDA PADILLA
Estudiante de Pasantía

Revisado por

Ing. MAGRETH ROSSIO SANGUINO REYES
Director Proyecto

Evidencias para el Formato Checklist de Rango Seguridad Lógica PT. No. LV004

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

CONTROL PARA USUARIOS

PT. No. EF032

Figura 1. Lista de Usuarios SIIS

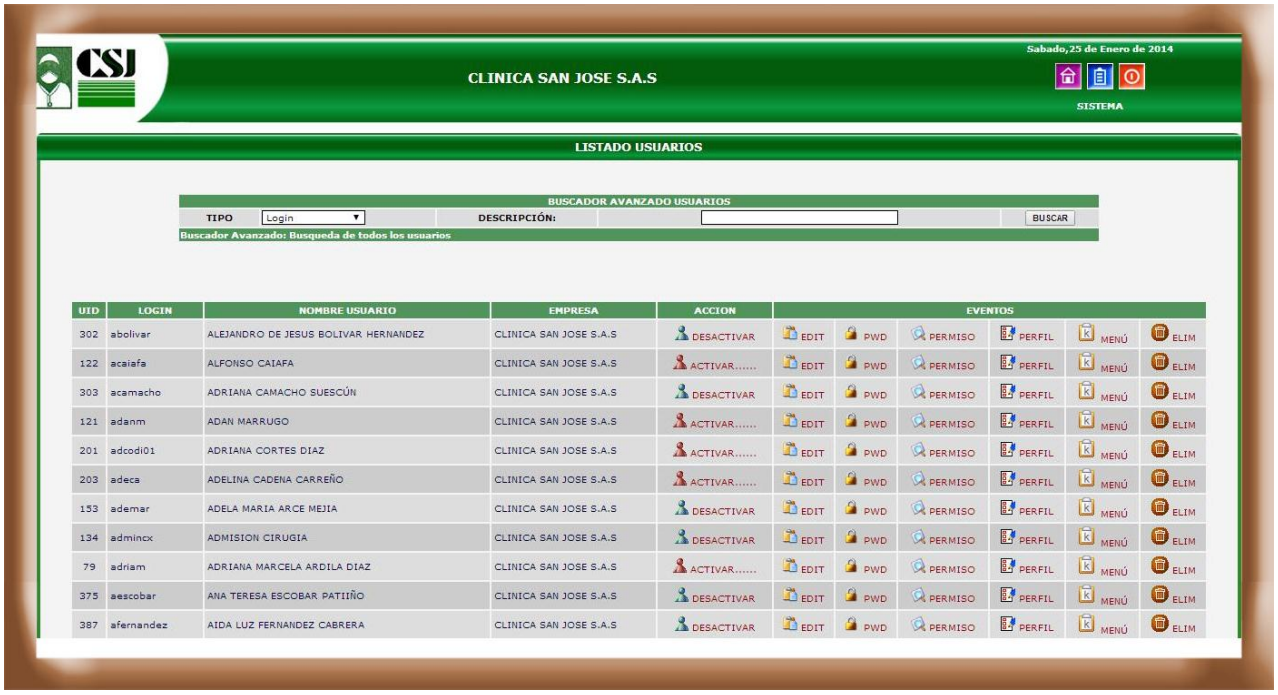
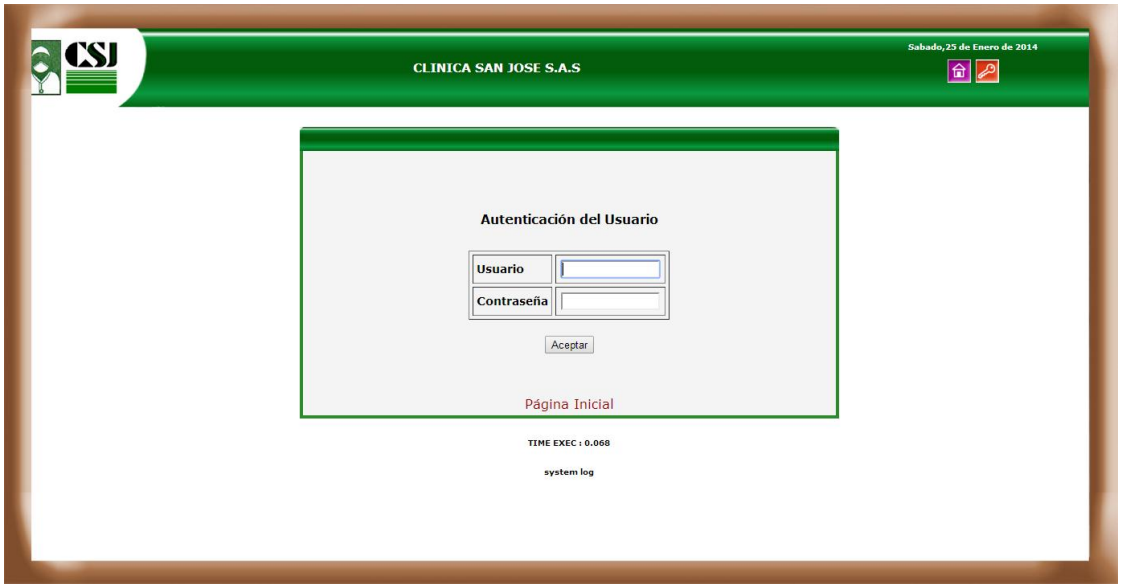
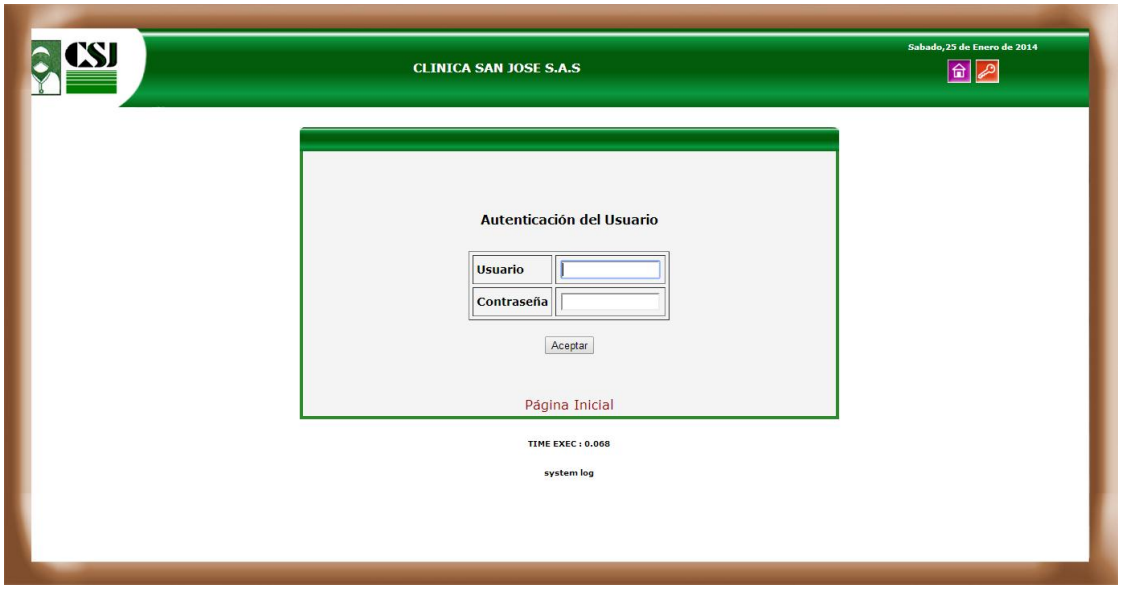


Figura 2. Menús del Usuario y Permisos

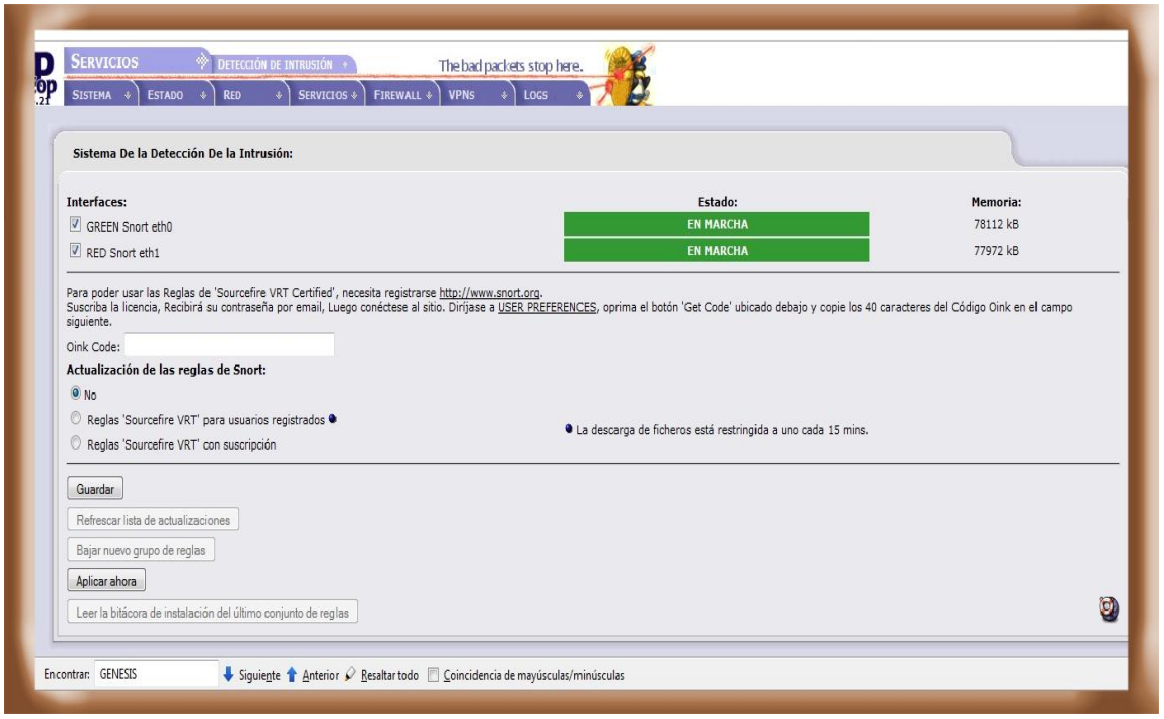
Figura 3. Logeo de Usuario



Evidencia Fotografía <u>EF033</u> para el formato Checklist de rango Seguridad Lógica



Evidencia Fotografía EF029 para el formato Checklist de rango Seguridad Lógica



Evidencia Fotografía EF030 para el formato Checklist de rango Seguridad Lógica

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

OPCIONES GENERALES PARA EL FILTRO DE URL (IPCOP)

PT. No. EF030

Figura 1. Filtro para URL

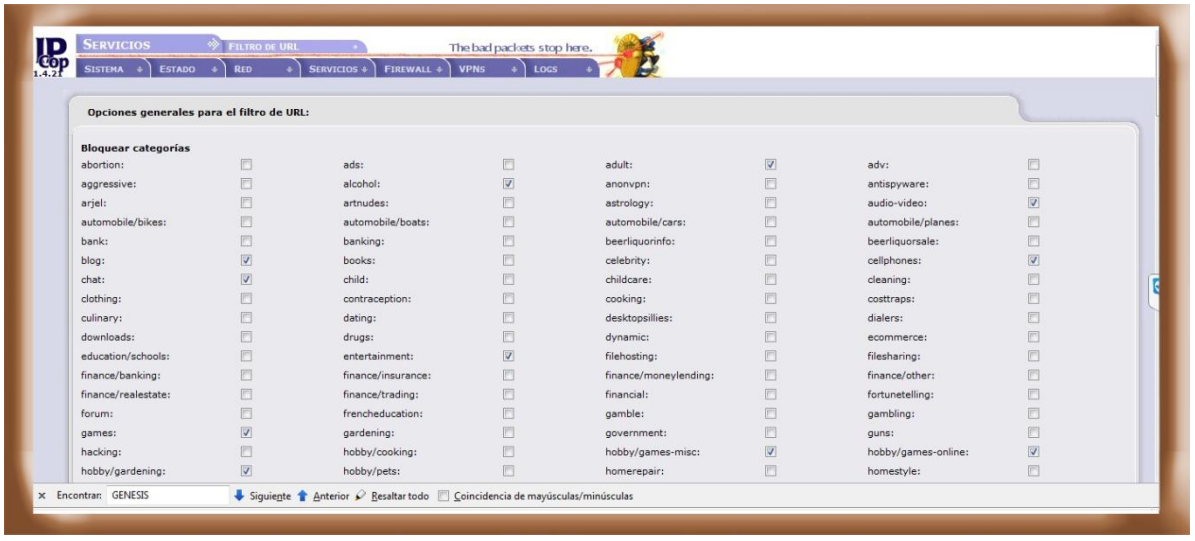


Figura 2. Bloque de servicios

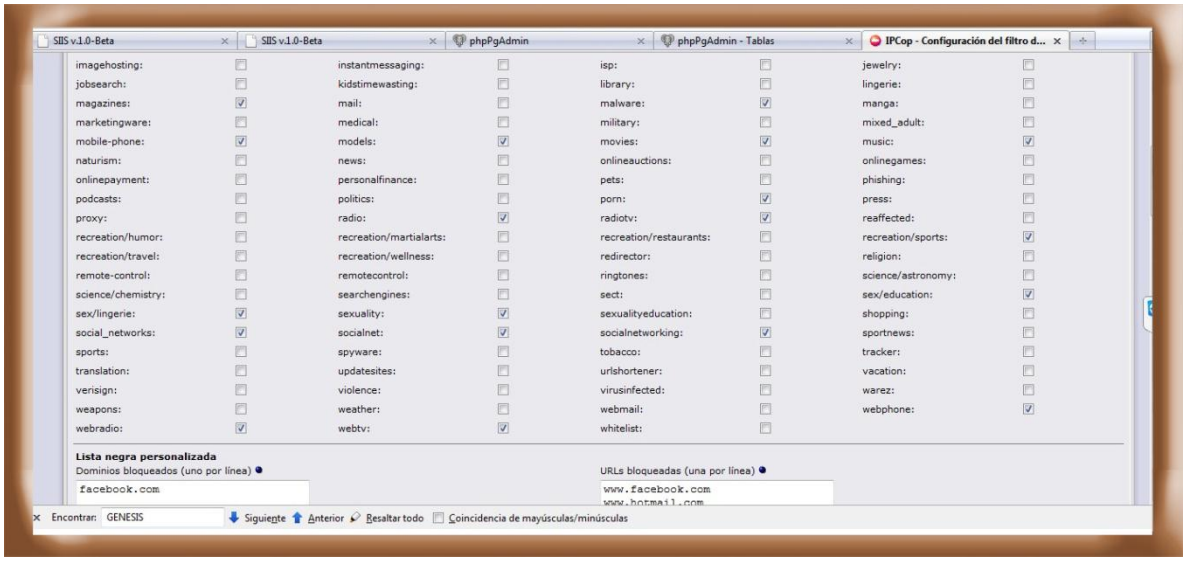


Figura 3. Bloqueo de plataformas web

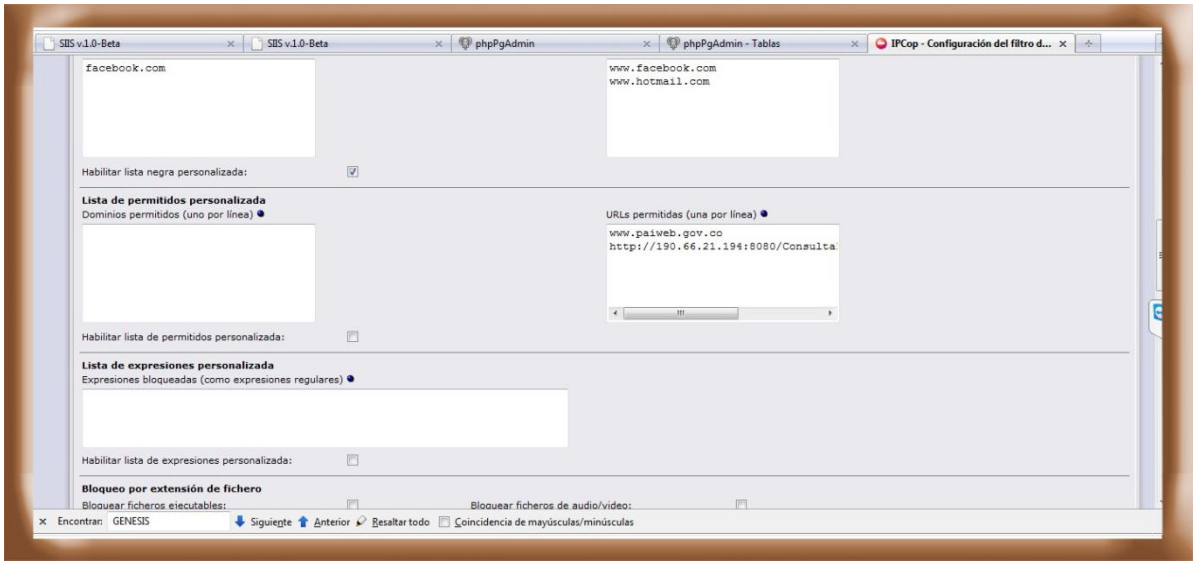


Figura 4. IP Fijas con permisos

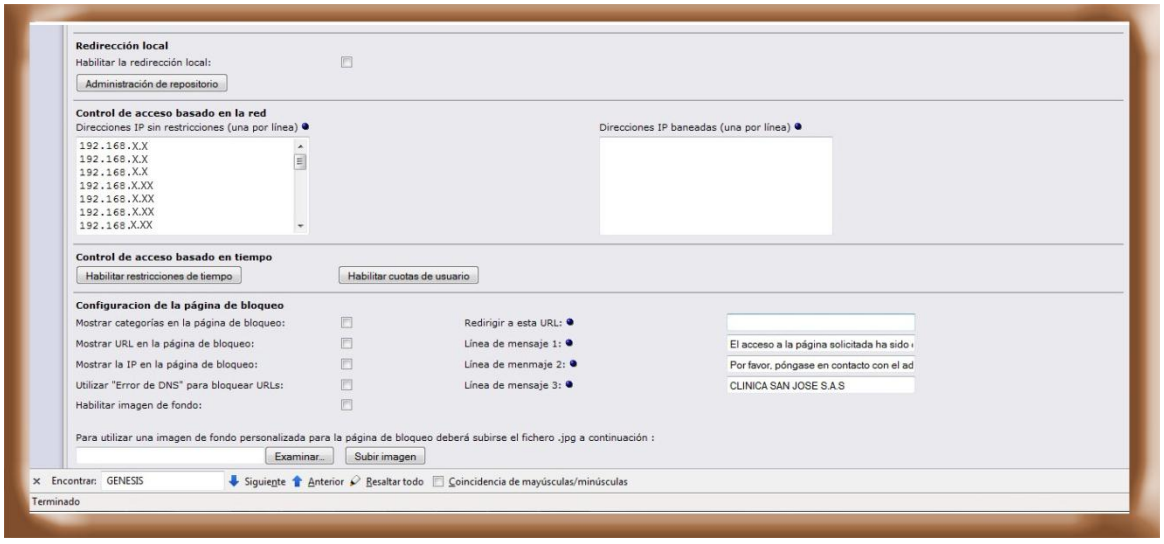
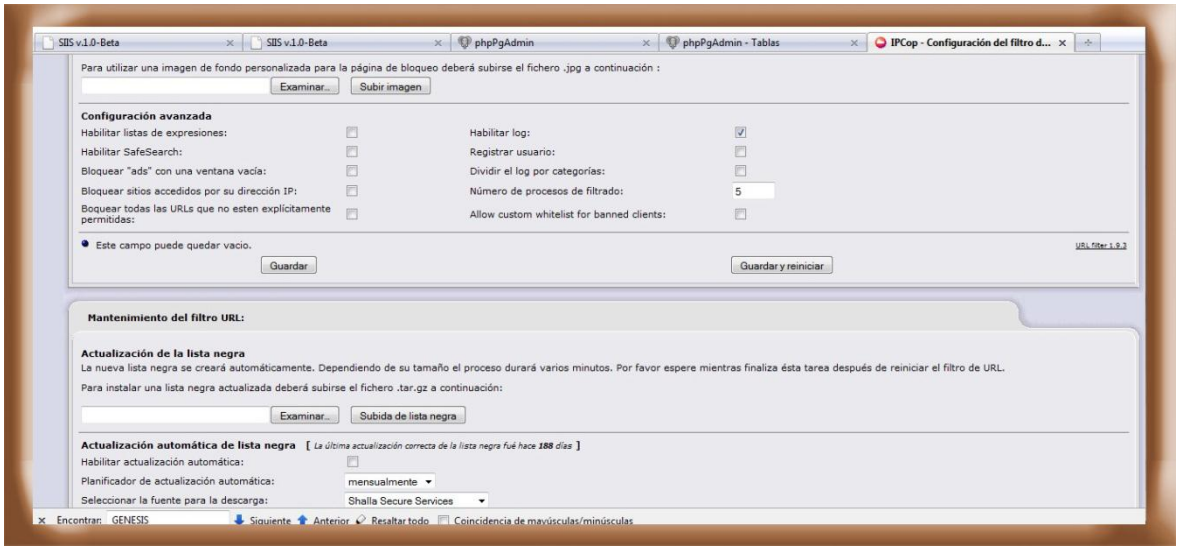


Figura 5. Configuraciones Avanzadas



Anexo K. Entrevista al Coordinador de Procesos para evaluar el servicio de mantenimiento de equipos

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

EN004

Objetivo: Evaluación del servicio de mantenimiento de hardware de la Clínica San José S.A.S.

Entrevistado: Ing. Nicolás De La Torre

Cargo: **Coordinador de Procesos**

1) Especifique el tipo de contrato de mantenimiento de equipos de cómputo que se tiene en la Clínica San José S.A.S

No existe tal contrato ya que se tiene el personal que lo realiza.

2) ¿Cómo se lleva a cabo el programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?

Cada 6 meses se realizan los mantenimientos a todos los dispositivos.

3) ¿Cómo se verifica esta acción?

No se cumple ningun protocolo, pero se realizan conversaciones con el personal que realiza los mantenimientos y tambien se utiliza la tecnica de la observación.

4) ¿Cómo se dan los tiempos de respuesta y de compostura en caso de fallas en los equipos de cómputo?

Apenas Ocurre alguna novedad, Inmediatame
el personal encargado toma cartas en el asun

5) ¿Cómo se notifican las fallas?

Verbalmente el personal de mantenimiento da
aviso al jefe inmediato y se produce la ejecución
actividades.

6) ¿Cómo se les da seguimiento?

Se le pregunta al personal de trabajo por l
continuas fallas que puedan estar Sucediendo.

7) ¿Se cuenta con un inventario de todos los equipos de cómputo que soportan la función informática de la Clínica?

Si, Ver inventario Sistemas.

8) ¿Con qué frecuencia se revisa el inventario?

No se lleva a cabo tal acción, Solo se
realizan notificaciones de cambios o fallas

9) ¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?

NO se lleva control.

10) ¿Se cuenta con servicio de mantenimiento para todos los equipos, incluyendo impresoras?

Si

11) ¿Con qué frecuencia se realiza mantenimiento a los equipos?

Cada 6 meses.

12) ¿Qué políticas tiene la Clínica para el proceso de adquisición de nuevos equipos?

Política como tal no existe, hasta que el equipo cumpla su vida útil

13) ¿Se tiene inventario actualizado de los equipos y terminales con su localización?

Si, Ver inventario Sistemas.

14) ¿Existe seguros o pólizas para la protección de los equipos de cómputo?

NO.

ENTREVISTADO
NICOLAS DE LA TORRE
Coordinador de Procesos

Henry Marulanda P.

ENTREVISTADOR
HENRY MARULANDA PADILLA
Estudiante Pasantía

Anexo K1. Formato Checklist de Rango

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

CHECKLIST DE RANGO

ENTIDAD: CLINICA SAN JOSE S.A.S. **PT. No. LV003**
Área: Mantenimiento de Equipos

Elaboró: H.M.P. **Fecha: 16-09-2013**
Revisó: M.R.S.R. **Fecha: 18-09-2013**
Aplicó: H.M.P. **Fecha: 29-09-2013**

Aplicado a: Ing. Nicolás De La Torre – Coordinador de Procesos
Objetivo: Evaluación del servicio de mantenimiento de hardware de la Clínica San José S.A.S.

ÍTEM	PREGUNTA	E	B	R	I	R/PT
1.	Especifique el tipo de contrato de mantenimiento de equipos de cómputo que se tiene en la Clínica San José S.A.S	X				
2.	¿Cómo se lleva a cabo el programa de mantenimiento preventivo para cada dispositivo del sistema de cómputo?		X			
3.	¿Cómo se verifica esta acción?			X		
4.	¿Cómo se dan los tiempos de respuesta y de compostura en caso de fallas en los equipos de cómputo?	X				
5.	¿Cómo se notifican las fallas?		X			
6.	¿Cómo se les da seguimiento?			X		
7.	¿Se cuenta con un inventario de todos los equipos de cómputo que soportan la función informática de la Clínica?	X				IE001
8.	¿Con qué frecuencia se revisa el inventario?		X			
9.	¿Se lleva un control de los equipos en garantía, para que a la finalización de ésta, se integren a algún programa de mantenimiento?				X	
10.	¿Se cuenta con servicio de mantenimiento para todos	X				

	los equipos, incluyendo impresoras?					
11.	¿Con qué frecuencia se realiza mantenimiento a los equipos?		X			
12.	¿Qué políticas tiene la Clínica para el proceso de adquisición de nuevos equipos?			X		
13.	¿Se tiene inventario actualizado de los equipos y terminales con su localización?	X				IE001
14.	¿Existen seguros o pólizas para la protección de los equipos de cómputo?				X	

H.M.P.: Henry Marulanda Padilla
M.R.S.R.: Magreth Rossio Sanguino Reyes – Director Proyecto
LV003.: Checklist de Rango No. 3
E: Excelente = 4
B: Bueno = 3
R.: Regular = 2
I.: Insuficiente = 1
R/PT: Referenciación de los Papeles de trabajo.
IE001: Inventario de equipos de cómputo

Después de aplicar el procedimiento de evaluación del Checklist para el servicio de mantenimiento de equipos, se obtuvo el siguiente resultado:
Cantidad de Ítem = 14

Ítem 1 = 4
Ítem 2 = 3
Ítem 3 = 2
Ítem 4 = 4
Ítem 5 = 3
Ítem 6 = 2
Ítem 7 = 4
Ítem 8 = 3
Ítem 9 = 1
Ítem 10 = 4
Ítem 11 = 3
Ítem 12= 2
Ítem 13 = 4
Ítem 14 = 1

Subtotal = Σ Item 1 hasta Item 14
Subtotal = 40
Total = Subtotal / Cantidad de ítems
Total = 40 / 14
Total = 2.86 ≈ 3 .0

Se puede concluir de acuerdo con los resultados obtenidos, que el servicio de Mantenimiento de Equipos de Cómputo de la Clínica San José S.A.S., es **Bueno**, ya que cuenta con procedimientos inmediatos de atención a la notificación de cualquier evento irregular en el funcionamiento de los mismos, lo que hace que los servicios soportados por dichos equipos de cómputo sean eficientes. Sin embargo, se evidenció, la carencia de procedimientos formales de protección de equipos.

Evaluado por

HENRY MARULANDA PADILLA
Estudiante de Pasantía

Revisado por

Ing. MAGRETH ROSSIO SANGUINO REYES
Director Proyecto

Evidencia para el Formato Checklist de Rango PT. No. LV003

CLINICA SAN JOSE S.A.S

INVENTARIO DE SISTEMAS

PT No. IE001

DEPARTAMENTO: Centro Ambulatorio

N. INVENTARIO	DESCRIPCION	REFERENCIA	MARCA	AREA
2273	Teclado	Kb-0316	HP	Recep Cent Ambulatorio
2275	CPU	Xl808av#219	HP	Recep Cent Ambulatorio
2276	Monitor	Hplv1911	HP	Recep Cent Ambulatorio
2277	Mouse	M-s0005-0	HP	Recep Cent Ambulatorio
1748	Impresora	Photo smart c4280	HP	Recep Cent Ambulatorio
1599	Teclado	K639	GENIUS	Fact Cent Ambulatirio
126	CPU	Clon	CLON	Fact Cent Ambulatirio
93	Monitor	Hsg 1044	QBEX	Fact Cent Ambulatirio
2279	Mouse	Xscroll	GENIUS	Fact Cent Ambulatirio
1340	Impresora	Laserjet P2055dn	HP	Fact Cent Ambulatirio
2278	Scaner	scanjet professional 1000	HP	Fact Cent Ambulatirio
2519	Teclado	BAUVTOBHH1A0NL	HP	Vacunacion
105	CPU	Kronos 5810290	QBEX	Vacunacion
104	Monitor	Hsg 1044	QBEX	Vacunacion
2282	Mouse	1f3f72d	QBEX	Vacunacion
782	Teclado	K9852	Delux	Consultorio 2
2283	CPU	Kronos 5810290	QBEX	Consultorio 2
89	Monitor	Hsg 1044	QBEX	Consultorio 2
115	Mouse	1f3f72d	QBEX	Consultorio 2
119	Teclado	KB-1000	OMEGA	Consultorio 3

109	CPU	Kronos 5810290	QBEX	Consultorio 3
117	Monitor	Hsg 1044	QBEX	Consultorio 3
2280	Mouse	Net scroll 120	GENIUS	Consultorio 3
1788	Teclado	Kb-06xe	QBEX	Fisioterapia
145	CPU	CLON	CLON	Fisioterapia
445	Monitor	T71w	BENQ	Fisioterapia
2281	Mouse	Gm-03022p	GENIUS	Fisioterapia
DEPARTAMENTO: Mantenimiento				
2284	Teclado	K639	GENIUS	Mantenimiento
2237	CPU	CLON	CLON	Mantenimiento
103	Monitor	Hsg 1044	QBEX	Mantenimiento
2285	Mouse	Net scroll 120	GENIUS	Mantenimiento
DEPARTAMENTO: Cuarto Piso UCI				
2138	Teclado	Kb-0316	HP	Equipo 1
2137	CPU	MXL2181JRP	HP	Equipo 1
2136	Monitor	LV1911	HP	Equipo 1
2139	Mouse	S-0005O	HP	Equipo 1
2142	Teclado	KB-0316	HP	Equipo 2
2141	CPU	MXL2180C27	HP	Equipo 2
2140	Monitor	LV1911	HP	Equipo 2
2143	Mouse	60053-002	HP	Equipo 2
DEPARTAMENTO: Tercer Piso				
2286	Teclado	KB-06XE	GENIUS	Enfermeria Equipo 1
1306	CPU	CLON	CLON	Enfermeria Equipo 1
2172	Monitor	T71W	DENQ	Enfermeria Equipo 1
2287	Mouse	Gm-03022p	GENIUS	Enfermeria Equipo 1
2175	Teclado	KB-0316	HP	Enfermeria Equipo 2
2288	CPU	COMPAQ 400 PRO SFF	HP	Enfermeria Equipo 2
2289	Monitor	LV1911	HP	Enfermeria Equipo 2
2176	Mouse	600553-002	HP	Enfermeria Equipo 2
1412	IMPRESORA	Laserjet P2055dn	HP	Enfermeria Equipo 2
2587	Teclado	Kb-110x	GENIUS	Facturacion
2198	CPU	Kronos 5810290	QBEX	Facturacion
2290	Monitor	Hsg 1044	QBEX	Facturacion
1016	Mouse	537750-001	GENIUS	Facturacion

DEPARTAMENTO: Segundo Piso				
1472	Teclado	KB-1000	OMEGA	Fact Cirugia
446	CPU	CLON	CLON	Fact Cirugia
2291	Monitor	Hsg 1044	QBEX	Fact Cirugia
1854	Mouse		Next	Fact Cirugia
2292	Impresora	F7bf031569	EPSON	Fact Cirugia
1474	Impresora	Laserjet P2055dn	HP	Fact Cirugia
128	Teclado	KB-1000	OMEGA	Enfermeros
2293	CPU	CLON	CLON	Enfermeros
118	Monitor	Hsg 1044	QBEX	Enfermeros
2485	Mouse	JW-cskm02	JAWAN	Enfermeros
1074	Computador Portatil	Presario C700	COMPAQ	Cirugia
2294	Computador Portatil	Aspire 4739	.ACER	Cirugia
2295	Teclado	K639	GENIUS	Cirugia
1335	CPU	Blue Code	CLON	Cirugia
1533	Monitor	W1943SG-PF	LG	Cirugia
2225	Mouse	216125e	QBEX	Cirugia
DEPARTAMENTO: Primer Piso				
2236	Teclado	KU-0138	GENIUS	Fact Urgencias
1172	CPU	5050MT	COMPAQ	Fact Urgencias
1171	Monitor	HP Le1901W	HP	Fact Urgencias
1174	Mouse	537750-001	GENIUS	Fact Urgencias
2296	Impresora	Lase Jet pro 400 MPF	HP	Fact Urgencias
2298	Teclado	K639	GENIUS	Consultorio 1
2300	CPU	TWIN 36102901	QBEX	Consultorio 1
2297	Monitor	IH182APB	QBEX	Consultorio 1
2299	Mouse	GM-03022P	GENIUS	Consultorio 1
2301	Teclado	SK-8115	DELL	Consultorio 2
2303	CPU	KRONOS 5810290	QBEX	Consultorio 2
125	Monitor	T71W	BENQ	Consultorio 2
2302	Mouse	GM-03022P	GENIUS	Consultorio 2
2304	Estabilizador	IEN-AVER1006	NEW	Consultorio 2
2307	Teclado	K639	GENIUS	Triage

890	CPU	KRONOS 5810290	QBEX	Triage
2306	Monitor	IH182APB	QBEX	Triage
2305	Mouse	Net scroll 120	GENIUS	Triage
2106	Computador Portatil	3c275176w	TOSHIBA	Triage
1921	Teclado	Sk-8110	DELL	Estcn enfermeria Eq1
2310	CPU	KRONOS 5810290	QBEX	Estcn enfermeria Eq1
55	Monitor	IH182APB	QBEX	Estcn enfermeria Eq1
2309	Mouse	GM-03022P	GENIUS	Estcn enfermeria Eq1
2308	Impresora	Hp Laser Jet P2035n	HP	Estcn enfermeria Eq1
2311	Estabilizador	Propc	NIOMAR	Estcn enfermeria Eq1
2314	Teclado	K639	GENIUS	Estcn enfermeria Eq2
97	CPU	KRONOS 5810290	QBEX	Estcn enfermeria Eq2
2312	Monitor	Hsg 1044	QBEX	Estcn enfermeria Eq2
2313	Mouse	GM-03022P	GENIUS	Estcn enfermeria Eq2
1772	Teclado	K639	GENIUS	Rayos X
435	CPU	CLON	CLON	Rayos X
1117	Monitor	W1934SI	LG	Rayos X
2315	Mouse	GM-03022P	GENIUS	Rayos X
2316	Impresora	GK420T	ZEBRA	Rayos X
DEPARTAMENTO: Farmacia				
2319	Teclado	539130-161	HP	Equipo 1
2317	CPU	MXL202020v	HP	Equipo 1
2318	Monitor	S1933	HP	Equipo 1
2320	Mouse	265966-011	HP	Equipo 1
2321	Teclado	Kb-0316	HP	Equipo 2
2323	CPU	MXL218146L	HP	Equipo 2
151	Monitor	913FW	AOC	Equipo 2
2566	Mouse	jw- cskm 02	JAWAN	Equipo 2
DEPARTAMENTO: Apoyo Diagnostico				
2324	Teclado	Kb-0316	HP	Apoyo Diagnostico
2327	CPU	MXL218146L	HP	Apoyo Diagnostico
2325	Monitor	Lv1911	HP	Apoyo Diagnostico

2326	Mouse	537748-001	HP	Apoyo Diagnostico
1349	Impresora	Laserjet P2055dn	HP	Apoyo Diagnostico
1904	Scaner	scanjet professional 1000	HP	Apoyo Diagnostico
DEPARTAMENTO: Laboratorio				
2328	Teclado	164.960.304.851	GENIUS	Laboratorio
422	CPU	CLON	DELUX	Laboratorio
779	Monitor	HW173A	QBEX	Laboratorio
1107	Mouse			Laboratorio
DEPARTAMENTO: Administracion				
2330	Teclado	Kb-0316	HP	Archivo
2332	CPU	MXL218146L	HP	Archivo
2331	Monitor	Lv1911	HP	Archivo
2329	Mouse	60053-002	HP	Archivo
2333	Estabilizador		NEW LINE	Archivo
2334	CPU	CLON	CLON	Secrt Auxiliar
434	Monitor	PL-19b	PROVIEW	Secrt Auxiliar
2336	Mouse	GM-03022P	GENIUS	Secrt Auxiliar
2337	Teclado	539130-161	HP	Fact. Y Auditoria
2340	CPU	MXL1151D18	HP	Fact. Y Auditoria
2339	Monitor	S2021	CONPAQ	Fact. Y Auditoria
2338	Mouse	26598-011	HP	Fact. Y Auditoria
2341	Teclado	K639	GENIUS	Glosas
1601	CPU	CLON	CLON	Glosas
1598	Monitor	E1920NX	SANSUNG	Glosas
2342	Mouse	60053-003	HP	Glosas
2343	Teclado	Kb-0316	HP	Auditoria Coomeva
2345	CPU	MXL1151D18	HP	Auditoria Coomeva
159	Monitor	716Sw	AOC	Auditoria Coomeva
2344	Mouse	Net scroll 120	GENIUS	Auditoria Coomeva
1305	Teclado	K639	GENIUS	Aux Administrativa
2402	CPU	CLON	CLON	Aux Administrativa
2347	Monitor	Lv1911	HP	Aux Administrativa
2346	Mouse	Net scroll 120	GENIUS	Aux Administrativa

2350	CPU	MXL202020G	HP	secretaria
2349	Monitor	LV1911	HP	secretaria
2348	Mouse	265966-011	HP	secretaria
1024	Teclado	KB-1000	OMEGA	secretaria
1359	Computador Portatil	ASPIRE 5338	.Acer	Jefe de Sistemas
2351	Mouse	Net scroll 100x	GENIUS	Jefe de Sistemas
2352	Teclado	539130-161	HP	Envios
2354	CPU	MXL1151D00	HP	Envios
1631	Monitor	WM767A	COMPAQ	Envios
2353	Mouse	265966-011	HP	Envios
2356	Teclado	539130-161	HP	Director Administrativo
2357	CPU	MXL202020L	HP	Director Administrativo
2358	Monitor	XJ311A	HP	Director Administrativo
2355	Mouse	265966-011	HP	Director Administrativo
1173	Teclado	505130-011	HP	Gerente de Servicios
1634	CPU	MXL1011R6C	HP	Gerente de Servicios
1628	Monitor	S2021	COMPAQ	Gerente de Servicios
2359	Mouse	265986-011	HP	Gerente de Servicios
1629	Teclado	KB-1000	OMEGA	Salud Ocupacional 1
102	CPU	CLON	CLON	Salud Ocupacional 1
1212	Monitor	E170Sc	DELL	Salud Ocupacional 1
2360	Mouse	GM-03022P	GENIUS	Salud Ocupacional 1
2361	Estabilizador	Propc	NIOMAR	Salud Ocupacional 1
1301	Teclado	L-358c	QBEX	Salud Ocupacional 2
1211	CPU	CLON	CLON	Salud Ocupacional 2
2363	Monitor	E1942c-BN	LG	Salud Ocupacional 2
2362	Mouse	GM-03022P	GENIUS	Salud Ocupacional 2
2335	Teclado	53130-161X	HP	Aux Contable
2365	CPU	MXL1131BZ9	HP	Aux Contable
2366	Monitor	S2021	COMPAQ	Aux Contable
2364	Mouse	265986-011	HP	Aux Contable

2368	Teclado	KB-1000	OMEGA	Aux Tesoreria
2369	CPU	MXL2020217	HP	Aux Tesoreria
2370	Monitor	S1933	HP	Aux Tesoreria
2367	Mouse	265986-011	HP	Aux Tesoreria
2372	Teclado	CSS-720	PC SMART	Aux Cartera
2373	CPU		PC SMART	Aux Cartera
67	Monitor	HW173A	QBEX	Aux Cartera
2371	Mouse	CSS-720	PC SMART	Aux Cartera
2375	Teclado	K639	GENIUS	Contadora
149	CPU	CLON	CLON	Contadora
1308	Monitor	S19A300B	SANSUNG	Contadora
1663	Mouse	Net scroll 120	GENIUS	Contadora
2374	Impresora	LX-300+II	EPSON	Contadora
1720	Teclado	539130-161	HP	Gerencia
1723	CPU	MXL1611RSQ	HP	Gerencia
1719	Monitor	S2021	COMPAQ	Gerencia
1721	Mouse	265986-011	HP	Gerencia
DEPARTAMENTO: Avanzar				
415	Computador Portatil	ASPIRE 5338	.Acer	Odontologia Eqp 1
1317	Computador Portatil	ASPIRE 5338	.Acer	Odontologia Eqp 2
2376	Mouse	Xscroll	GENIUS	Odontologia Eqp 2
DEPARTAMENTO: Sistemas				
2221	Servidor	Power edge 2600	DELL	Sistemas
2222	Servidor	Power edge 2900	DELL	Sistemas
1030	Servidor	Power edge 2600	DELL	Sistemas
1046	Servidor	Power edge 1900	DELL	Sistemas
2223	UPS	Electra	QBEX	Sistemas
1013	UPS	Ecoserver ups	QUEST	Sistemas
2231	Rack	Super stack	3COM	Sistemas
2232	Dvr	tv-7216	Network dvr	Sistemas
76	Monitor	Hw 173a	QBEX	Sistemas
38	Monitor	Flatron ez t730sh	LG	Sistemas
1600	Mouse	Zmo 344	GENIUS	Sistemas
1075	Mouse	Um 2018	katec	Sistemas

87	Teclado	Y-UM76A	LOGITECH	Sistemas
144	Teclado	K639	GENIUS	Sistemas
1071	Radio	Pmn 4000d	MOTOROLA	Sistemas
1072	Radio	Pmn 4000d	MOTOROLA	Sistemas

Anexo L. Formato Checklist Binario para Evaluar Infraestructura de Red

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

CHECKLIST BINARIO

ENTIDAD: CLINICA SAN JOSE S.A.S. PT. No. LV002
Área: Infraestructura de la Red de Datos

Elaboró: H.M.P. Fecha: 20-09-2013
Revisó: M.R.S.R. Fecha: 25-09-2013
Aplicó: H.M.P. Fecha: 10-10-2013

Aplicado a: Ing. Nicolás De La Torre – Coordinador de Procesos
Objetivo: Evaluar los recursos de seguridad física de la Red de Datos de La Clínica San José S.A.S

ÍTEM	PREGUNTA	EXISTE		R/PT
		SI	NO	
1.	¿Existe la etiquetación de nodos apegada al estándar 802.11g para la reducción de velocidad de transmisión?		X	
2.	¿El cableado está certificado?		X	
3.	¿El cableado en el interior y exterior del edificio lleva a un cuarto de equipos o armario de telecomunicaciones?	X		EF018
4.	¿Se cuenta con Switch adicional en caso de fallo?	X		
5.	¿El armado del cable cumple con el estándar de red?		X	EF019
6.	¿El armado del Patch panel cumple con un estándar de red?		X	
7.	¿Existe una separación entre los equipos y el cuarto de telecomunicaciones?	X		
8.	¿Esta implementado un mapa del sembrado de nodos?		X	
9.	¿Existe mapa de rutas de red?		X	
10.	¿Cuenta con una red específica para la transmisión de voz, datos y video?		X	
11.	¿El cableado del edificio viaja dentro de canaleta o ducto?		X	
12.	¿Cuenta con dispositivo de seguridad para la red?		X	
13.	¿Usa dirección IP'S manuales?	X		EF023
14.	¿Usa direcciones IP'S automáticas?	X		EF024

15.	¿Se cuenta con UPS para los equipos como router, switch, modem?	X		EF020
16.	¿Cuenta con espacio adicional el rack para seguir colocando dispositivos?	X		
17.	¿Cuenta con la última categoría de cableado?		X	
18.	¿Cuenta con voltaje regulado?	X		
19.	¿Existe fibra óptica en algún punto de la red?	X		EF021
20.	¿Está restringido el acceso a los router?	X		
21.	¿Los Access Point's usan encriptación de 64, 128 o 256 bits?	X		
22.	¿Los Access Point cuentan con seguridad?	X		
23.	¿Se cuenta con un cuarto de telecomunicaciones?	X		EF026
24.	¿Se realizan actualizaciones a los mapas físicos y lógicos de la red?		X	
25.	¿Existe un registro de eventos de los usuarios que acceden a la red?		X	
26.	¿Existe una persona encargada de la administración de la red?	X		
27.	¿La red está protegida contra los intrusos activos (hackers, crackers, entre otros.)?	X		EF025
28.	¿El cableado de red se encuentra separado del cableado eléctrico?		X	
29.	¿Las terminaciones del cable de red cuentan con instalaciones adecuadas, es decir con nodos elaborados?		X	
30.	¿Utiliza cableado sobre techo falso?	X		EF027
31.	¿La red es compartida por otros edificios?		X	
32.	¿Las terminaciones o jack's de los nodos están configurados bajo el estándar T568-B?	X		
33.	En caso de no cubrir toda el área deseada ¿cuentan con repetidores de señal?	X		
35.	¿Existe una tabla de direccionamiento?	X		
36.	¿Se cuenta con las herramientas necesarias para la elaboración de los cables de red y montaje de la misma?	X		
37.	¿De acuerdo con los diversos tipos de servicios (voz, datos, etc.) los cables están divididos conforme al servicio que brindan?		X	

A nivel de infraestructura de la red de datos, se puede concluir que la clínica tiene implementados algunos mecanismos de seguridad física y lógica que permiten mantener un cierto grado de confidencialidad de la información que viaja o se transmite a través de la red de datos y para dar soporte a los servicios ofrecidos por la clínica.

Por su parte, la evaluación de dicho aspecto a través del Checklist binario, permite evidenciar que aquellos ítems marcados con **NO** (0) corresponden a aspectos negativos que pueden poner en riesgo la seguridad, integridad y disponibilidad de la información.

H.M.P.: Henry Marulanda Padilla
M.R.S.R.: Magreth Rossio Sanguino Reyes – Director Proyecto
LV002: Checklist Binario No. 2.
R/PT: Referenciación de los Papeles de trabajo
EF018-EF019-EF020-EF021-EF023-EF024-EF025-EF026-EF027: Evidencias fotográficas

Aplicado por:

Henry Marulanda P.

HENRY MARULANDA PADILLA
Estudiante de Pasantía

Aplicado a:

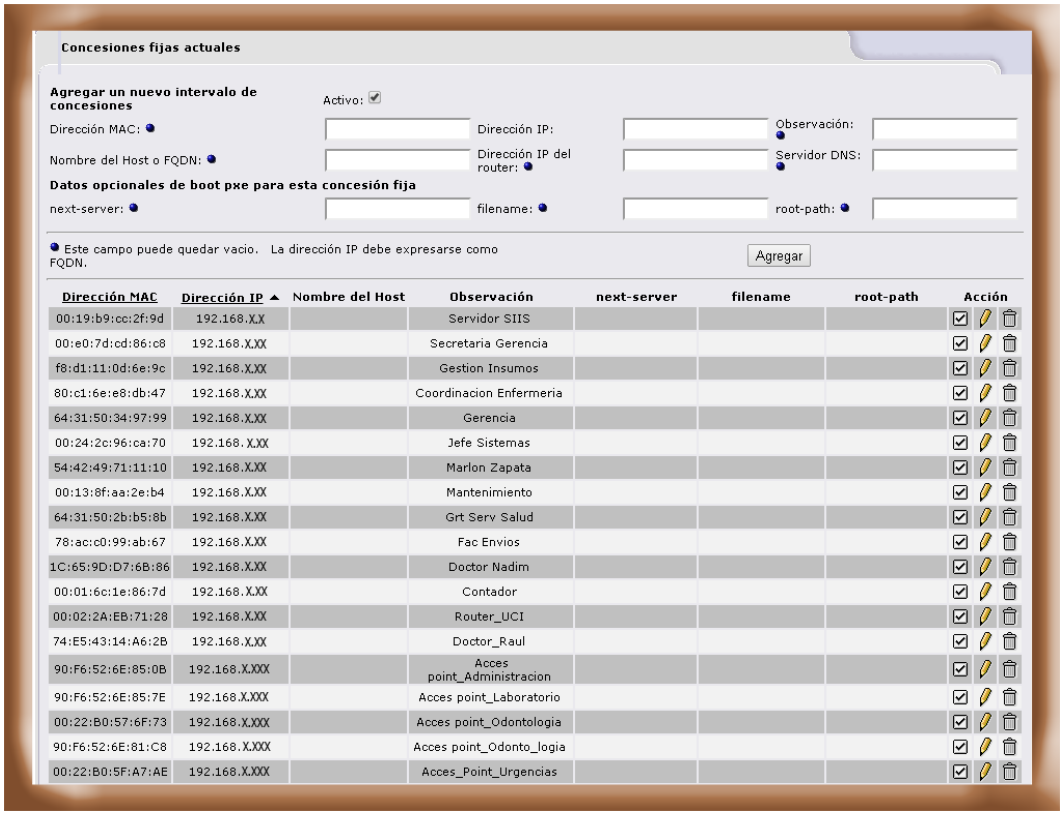
NICOLÁS DE LA TORRE VILLLARREAL
Coordinador de Procesos

Evidencias para el Formato Checklist Binario PT. No. LV002

Foto EF018. Cableado dirigido hacia el cuarto de comunicaciones

Foto <u>EF019</u>. Switch Adicionales

Figura EF023. Direcciones IP Manuales



Concesiones fijas actuales

Agregar un nuevo intervalo de concesiones Activo:

Dirección MAC: Dirección IP: Observación:

Nombre del Host o FQDN: Dirección IP del router: Servidor DNS:

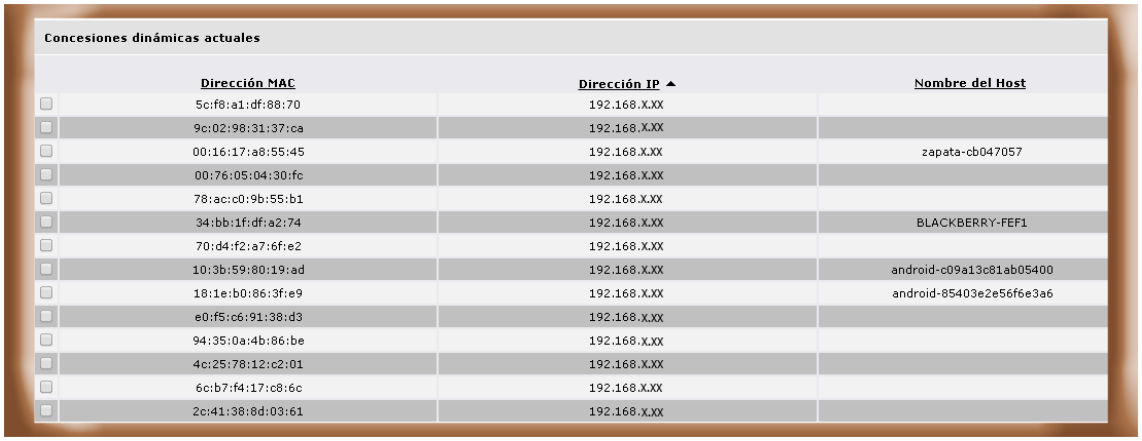
Datos opcionales de boot pxe para esta concesión fija

next-server: filename: root-path:

Este campo puede quedar vacio. La dirección IP debe expresarse como FQDN. Agregar

Dirección MAC	Dirección IP	Nombre del Host	Observación	next-server	filename	root-path	Acción
00:19:b9:cc:2f:9d	192.168.X.X		Servidor SIIS				
00:e0:7d:cd:86:c8	192.168.X.XX		Secretaria Gerencia				
f8:d1:11:0d:6e:9c	192.168.X.XX		Gestion Insumos				
80:c1:6e:e8:db:47	192.168.X.XX		Coordinacion Enfermeria				
64:31:50:34:97:99	192.168.X.XX		Gerencia				
00:24:2c:96:ca:70	192.168.X.XX		Jefe Sistemas				
54:42:49:71:11:10	192.168.X.XX		Marlon Zapata				
00:13:8f:aa:2e:b4	192.168.X.XX		Mantenimiento				
64:31:50:2b:b5:8b	192.168.X.XX		Grt Serv Salud				
78:ac:c0:99:ab:67	192.168.X.XX		Fac Envios				
1C:65:9D:D7:6B:86	192.168.X.XX		Doctor Nadim				
00:01:6c:1e:86:7d	192.168.X.XX		Contador				
00:02:2A:EB:71:28	192.168.X.XX		Router_UCI				
74:E5:43:14:A6:2B	192.168.X.XX		Doctor_Raul				
90:F6:52:6E:85:0B	192.168.X.XXX		Acces point_Administracion				
90:F6:52:6E:85:7E	192.168.X.XXX		Acces point_Laboratorio				
00:22:B0:57:6F:73	192.168.X.XXX		Acces point_Odontologia				
90:F6:52:6E:81:C8	192.168.X.XXX		Acces point_Odonto_logia				
00:22:B0:5F:A7:AE	192.168.X.XXX		Acces_Point_Urgencias				

Figura EF024. Direcciones IP Automáticas



Concesiones dinámicas actuales

Dirección MAC	Dirección IP ▲	Nombre del Host
5c:f8:a1:df:88:70	192.168.X.XX	
9c:02:98:31:37:ca	192.168.X.XX	
00:16:17:a8:55:45	192.168.X.XX	zapata-cb047057
00:76:05:04:30:fc	192.168.X.XX	
78:ac:c0:9b:55:b1	192.168.X.XX	
34:bb:1f:df:a2:74	192.168.X.XX	BLACKBERRY-FEF1
70:d4:f2:a7:6f:e2	192.168.X.XX	
10:3b:59:80:19:ad	192.168.X.XX	android-c09a13c81ab05400
18:1e:b0:86:3f:e9	192.168.X.XX	android-85403e2e56f6e3a6
e0:f5:c6:91:38:d3	192.168.X.XX	
94:35:0a:4b:86:be	192.168.X.XX	
4c:25:78:12:c2:01	192.168.X.XX	
6c:b7:f4:17:c8:6c	192.168.X.XX	
2c:41:38:8d:03:61	192.168.X.XX	

Foto EF020: UPS

Foto <u>EF021</u>: Fibra Óptica

Foto <u>EF026:</u> Cuarto de Telecomunicaciones

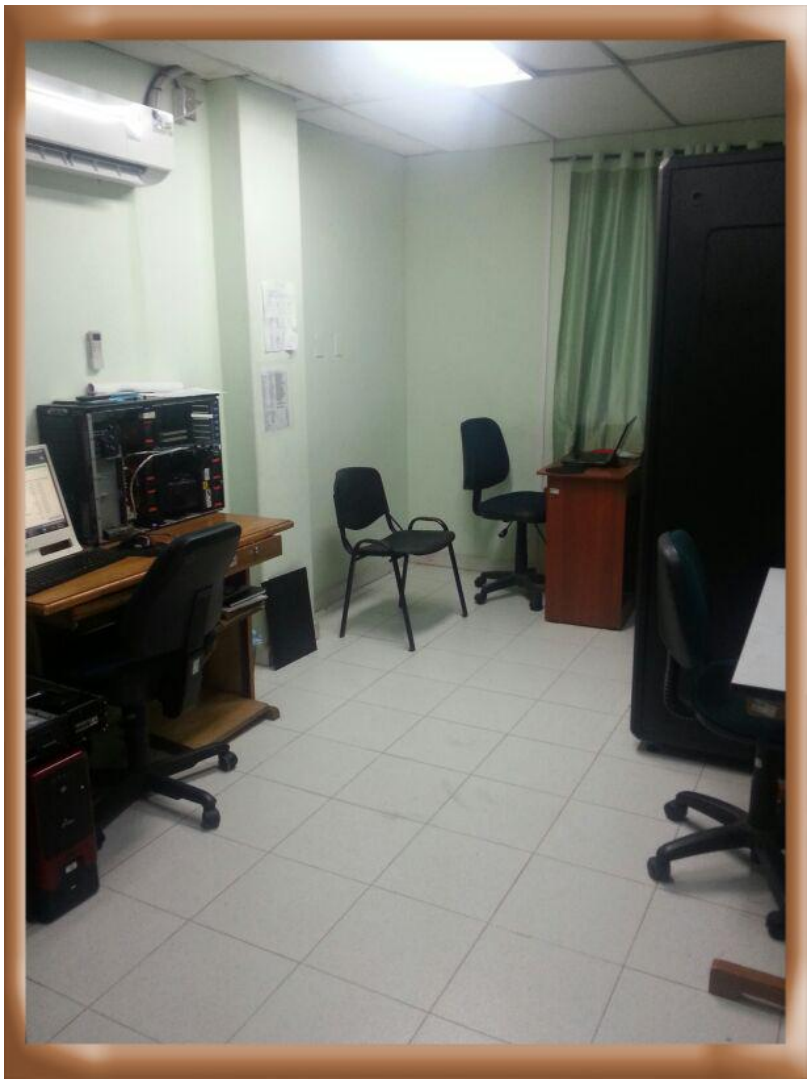
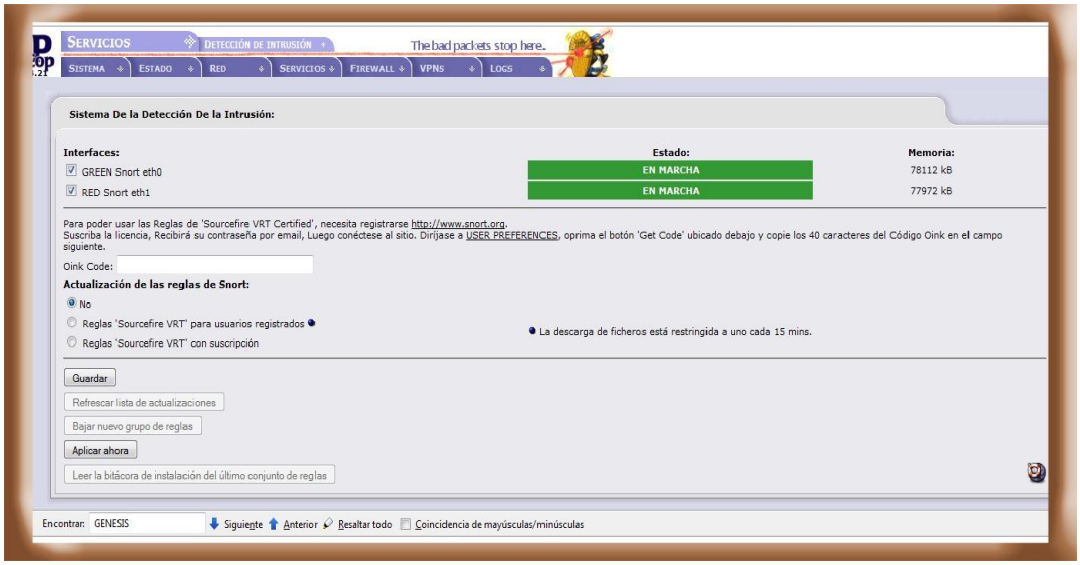


Figura EF025: Detección de Intrusos



CABLEADO SOBRE TECHO FALSO

PT. No. EF027

Foto 1. Cableado UTP Categoría 5E sobre techo falso Cuarto piso

Foto 2. Cableado UTP Categoría 5E sobre techo falso Tercer piso

Foto 3. Cableado UTP Categoría 5E sobre techo falso Segundo piso

Foto 4. Cableado UTP Categoría 5E sobre techo falso Primer piso

Anexo M. Entrevista al Administrador de la Base de Datos

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

EN006

Objetivo: Evaluación a la base de datos de la Clínica San José S.A.S

Entrevistado: **Ing. Cristhian Rodríguez**

Cargo: **Administrador Base de Datos**

1) ¿Las tablas maestras contienen índices creados?

Si, las tablas de parametros si los poseo.

2) ¿Qué actividades del negocio son soportadas por el sistema de información (Base de Datos)?

Historias clinicas, Facturación y Auditoria de cuentas medicas, cartera e informes.

3) ¿Qué políticas de seguridad posee la clínica para la base de datos?

Ninguna.

4) ¿Existen políticas de backup's? ¿Cuáles?

En el Manual de Archivos e historias clinicas.

5) ¿Existen roles de usuarios y privilegios a los mimos?

Si existen.

6) ¿Existen formatos de altas y bajas a usuarios (creación y eliminación de usuarios)? ¿Cómo se llevan a cabo?

No existen dichos formatos.

7) ¿Existen acuerdos de confidencialidad? ¿Cuáles?

NO.

8) ¿En caso de que el equipo principal donde está la base de datos falle existen equipos auxiliares?

Si existe equipos de respaldo.

9) ¿Está activa la auditoria automatizada a la DB?

Si.

Cristhian Sol R
ENTREVISTADO

Henry Haulanda P.
ENTREVISTADOR

Anexo N. Auditoria a la Base de Datos Clínica San José S.A.S

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

AUDITORIA A BASE DE DATOS

Alcance

El alcance de la Auditoría está definido por la Seguridad Lógica con el fin de determinar los controles de acceso a la base de datos y los mecanismos para determinar la integridad, confidencialidad y disponibilidad de la información.

NOTA:

Los nombres de las Tablas Maestras y Direcciones IP es informacion confidencial de la empresa, por tal motivo no serán revelas.

Tablas Maestras		
✓ inv_xxxxxx_xxxxxxxxxx	✓ tipo_dptos	✓ glosas_ xxxxxx _general
✓ inv_xxxxxx_xxxxxxxxxx	✓ tipo_id_texxxxxx	✓ glosas_xxxxx xx
✓ inv_xxx_xxx_anatofarmaco logico	✓ tipo_mxxxx	✓ grupos_xxxx xxxxxx
✓ inv_xxx_xxx_concentracion es	✓ tipo_xxxx	✓ subxxxxxx_t arifarios
✓ inv_medicamentos_xxxx_a dministracion	✓ tipo_xxxx	✓ grupos_xxxx x_cargo
✓ inv_subclases_xxxxxxxxxx	✓ tipos_adxxxxxxx	✓ diagxxxxxx x
✓ inv_unidades_xxxxxx_medi camentos	✓ tipos_xxxxxxx	✓ vias_inxxxxx
✓ notas_xxxxxx_ajuste_conce ptos	✓ tipos_fxxxxxxx	✓ causas_xxxx xxxx
✓ notas_xxxxxx_detalle_conc eptos	✓ tipos_xxxxxx	✓ tipos_cxxxxx x
✓ ocupaxxxxxx	✓ estaciones_enfermeria _xxxxxxxx	✓ rexxxxxxx
✓ os_xxxxxxx	✓ agenda_xxxxx_justific acion	✓ tipos_xxxxxx
✓ plan_taxxxxxxx	✓ autoxxxxxxxx_justific acion	
✓ puntos_admixxxxxx	✓ autorizaciones_tipos	
	✓ xxxxxxx_utilidad	
	✓ emxxxxxx	
	✓ tipos_xxx_bodega	

✓ puntos_facxxxxxxxx ✓ puntos_txxxxx ✓ qx_grupos_xxxxx_cargo ✓ qx_xxxxx_cirugia ✓ rc_conceptos_xxxxxxxxx ✓ rc_detalle_xxxxxxxxx_conceptos ✓ tarxxxxxxx ✓ terxxxxx	✓ conceptos_xxxx_conceptos ✓ cuentas_xxxxxxx ✓ cuxx ✓ dexxxxxxxxxx ✓ unidades_xxxxxxxxxx ✓ espexxxxxxxxx	✓ hc_xxxxx_finalidad

Se realizó un análisis de las tablas maestras utilizando el software **IDEA CaseWare 9.1, para detectar posibles campos duplicados en cada una de las tablas. A continuación, se muestran las imágenes que evidencian dicho proceso.**

Figura 1. Tabla grupos_tipxx_xxxxx

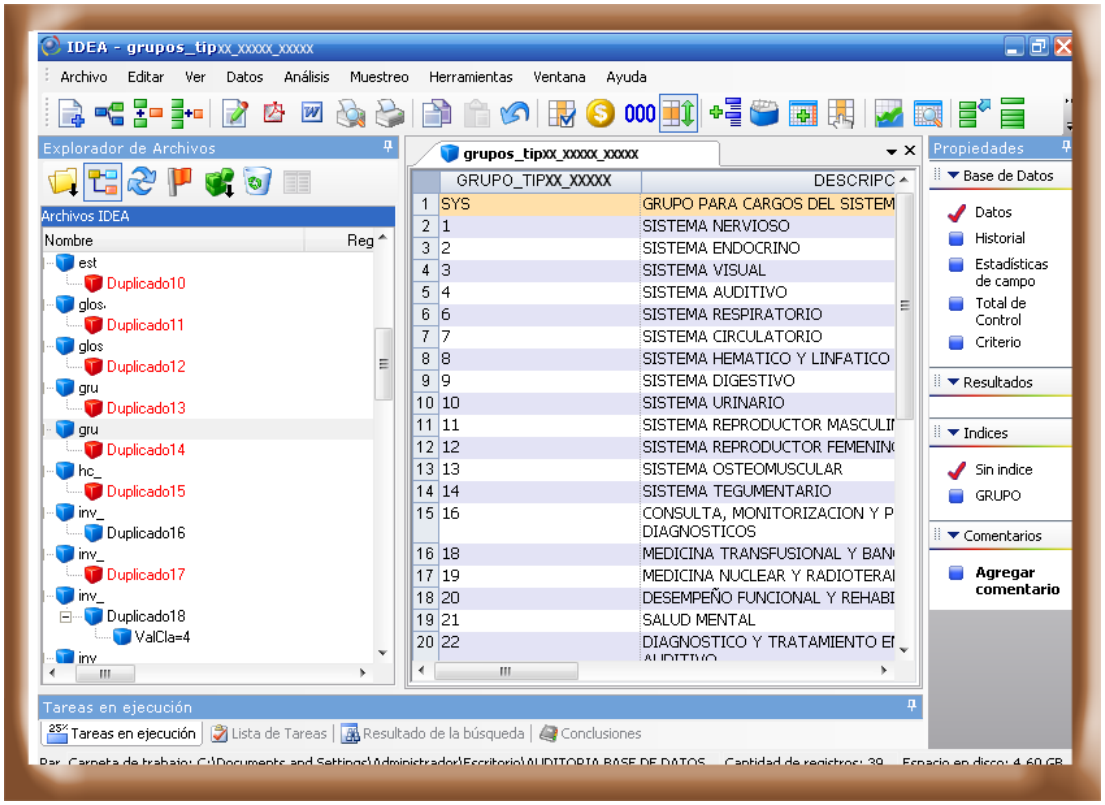


Figura 2. Generación de Duplicado

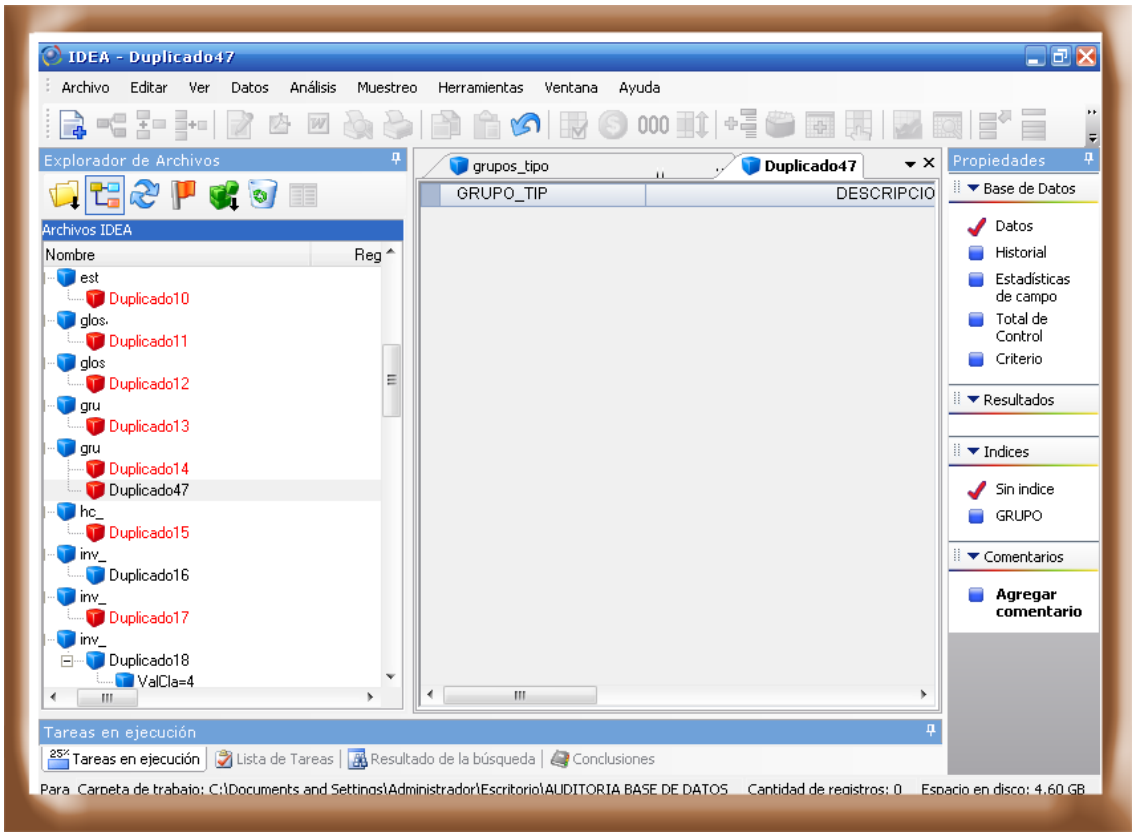


Figura 3. inv_m

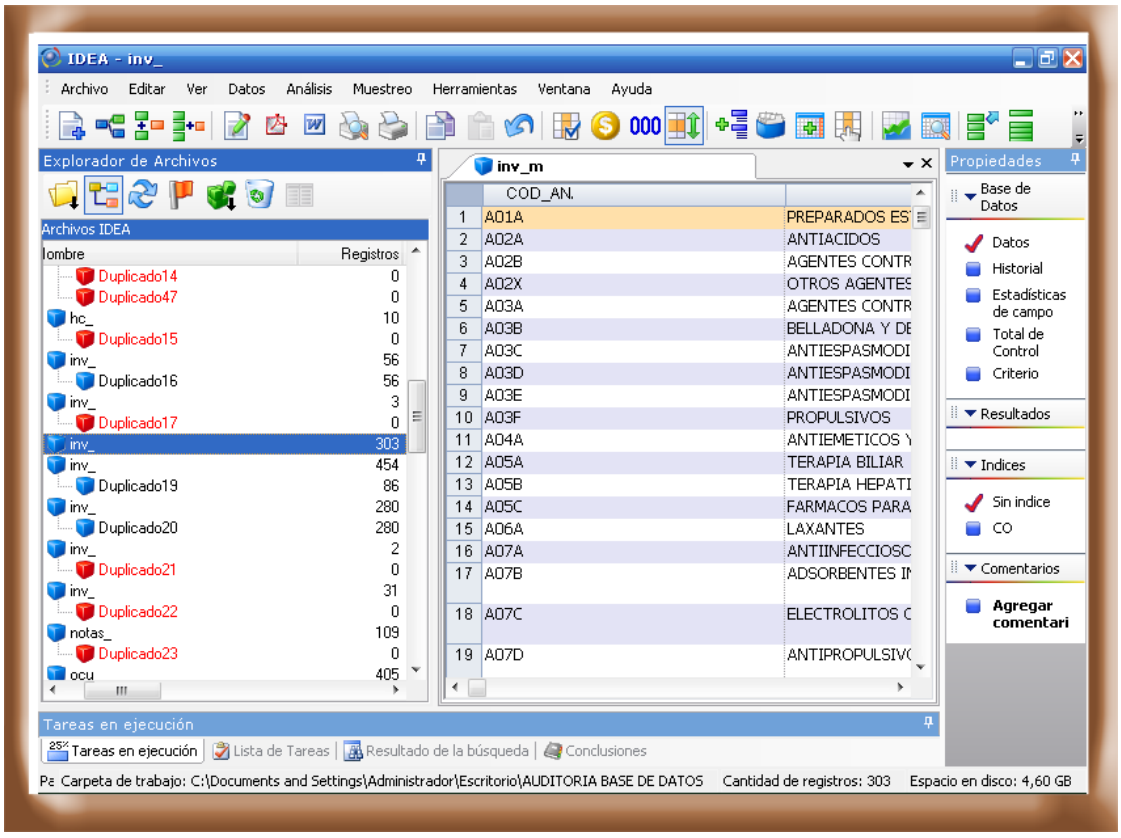


Figura 4. Generación de Duplicado

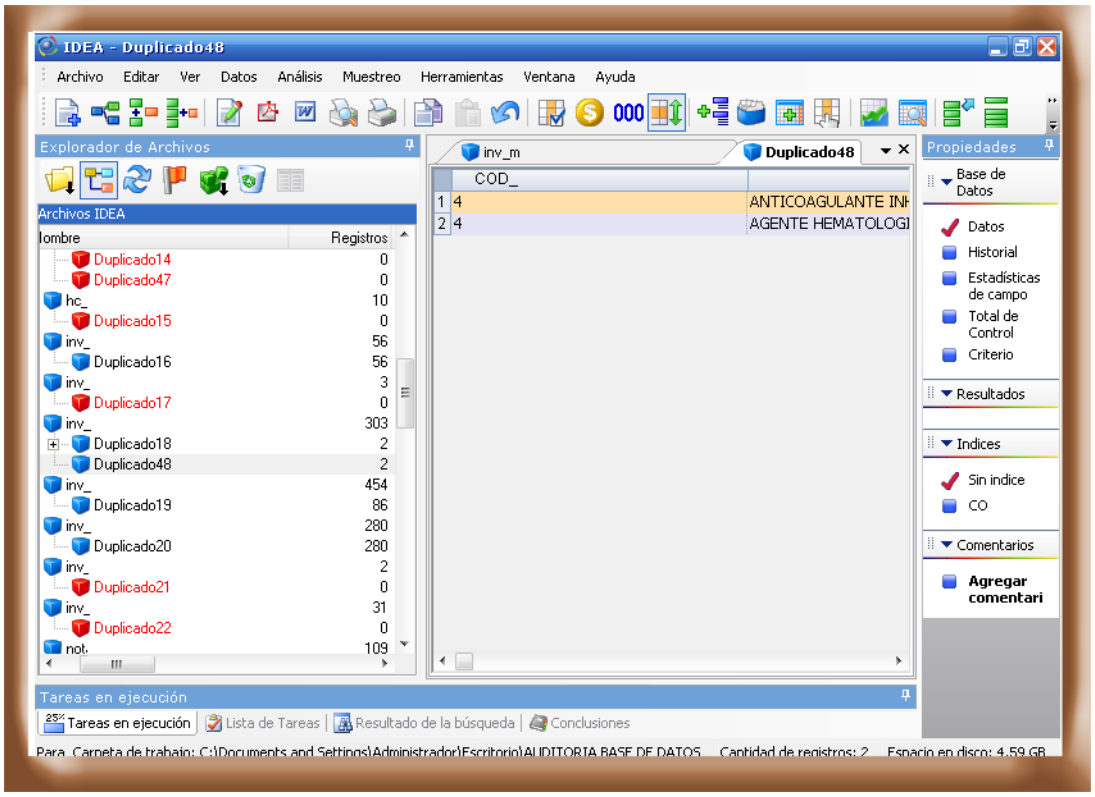


Figura 5. Tabla Cuxx

Realización de consulta SQL

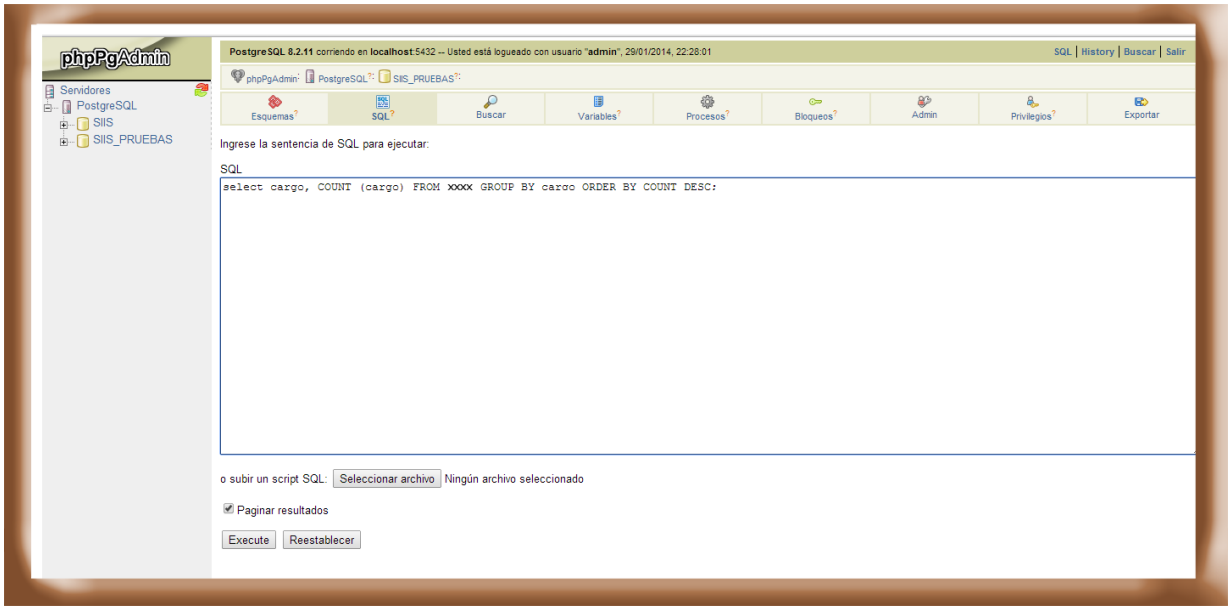


Figura 6. Resultado de la consulta

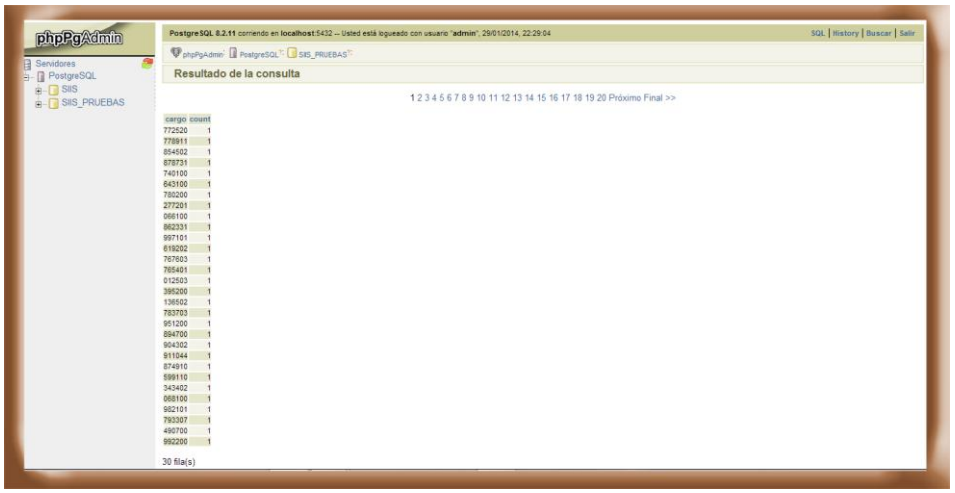


Figura 7. Tabla **diagxxxxxxxx**

Realización de consulta

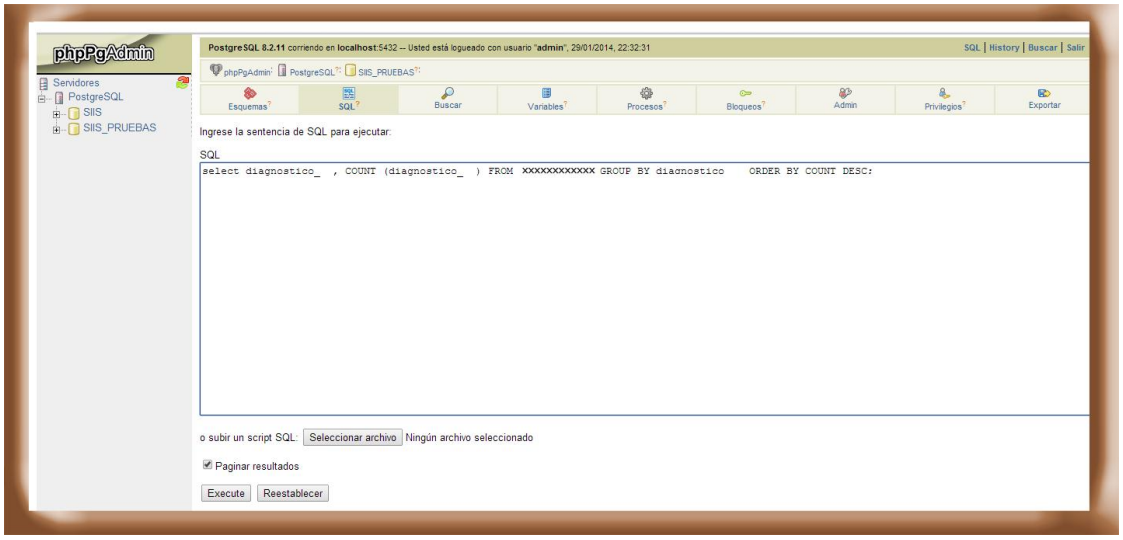


Figura 8. Resultado consulta

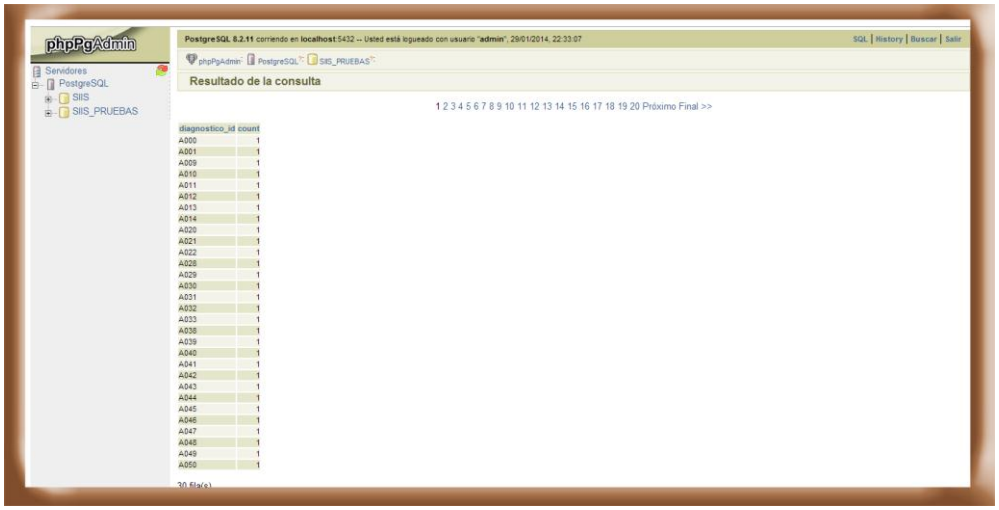


Figura 9. Tabla terxxxxx

Realización de consulta

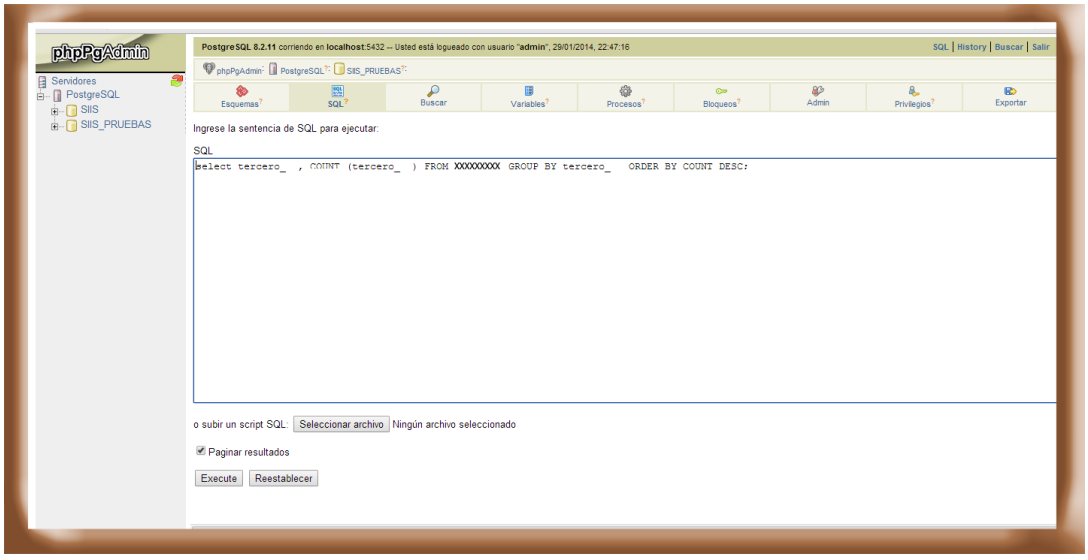


Figura 10. Resultado Consulta

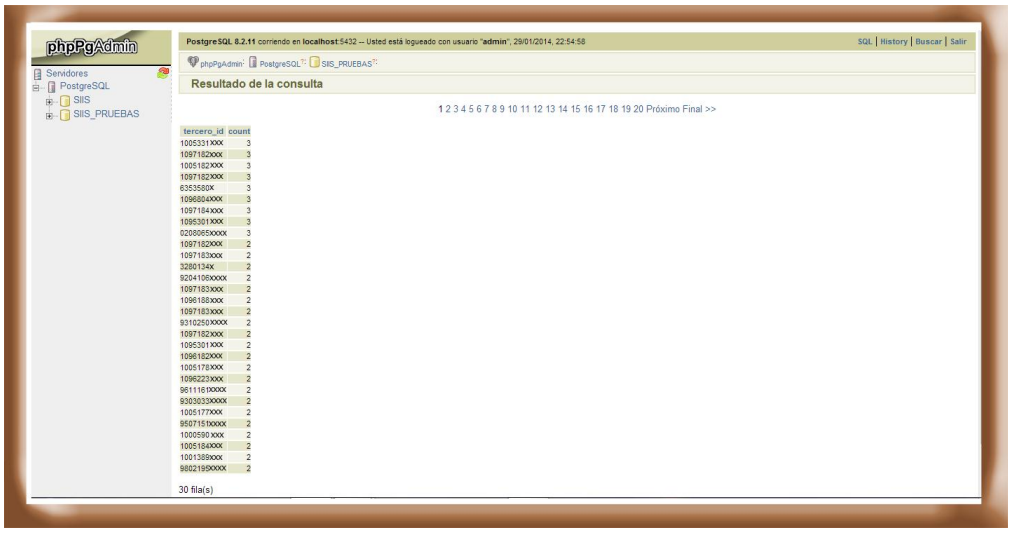
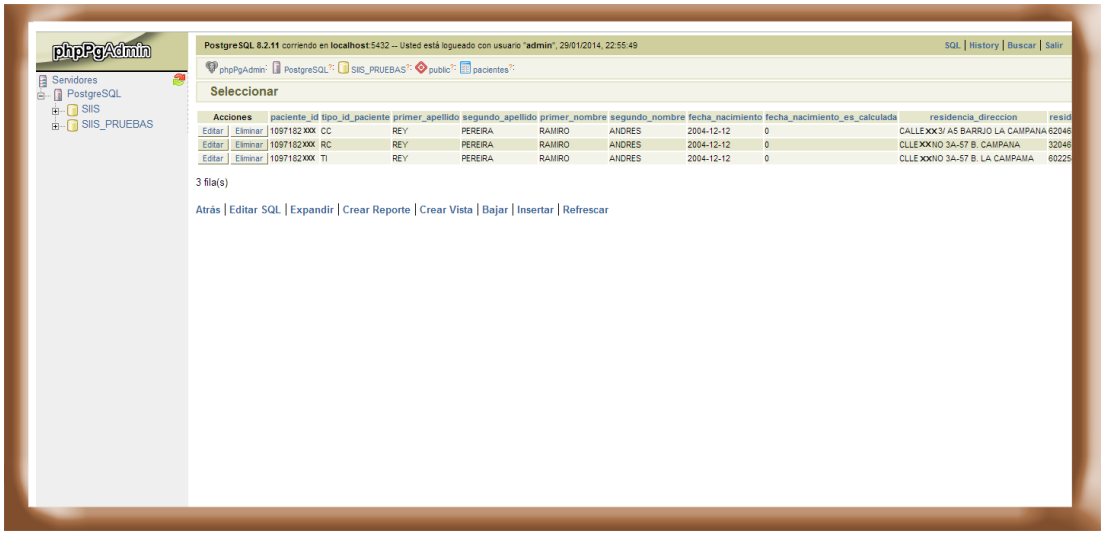


Figura 11. Visualización Duplicado



A pesar que la tabla paxxxxxx no hace parte de las tablas maestras, según argumento el administrador de la base de datos, se encontraron ciertas anomalías en ella.

Figura 12. Tabla paxxxxxx

Realización Consulta

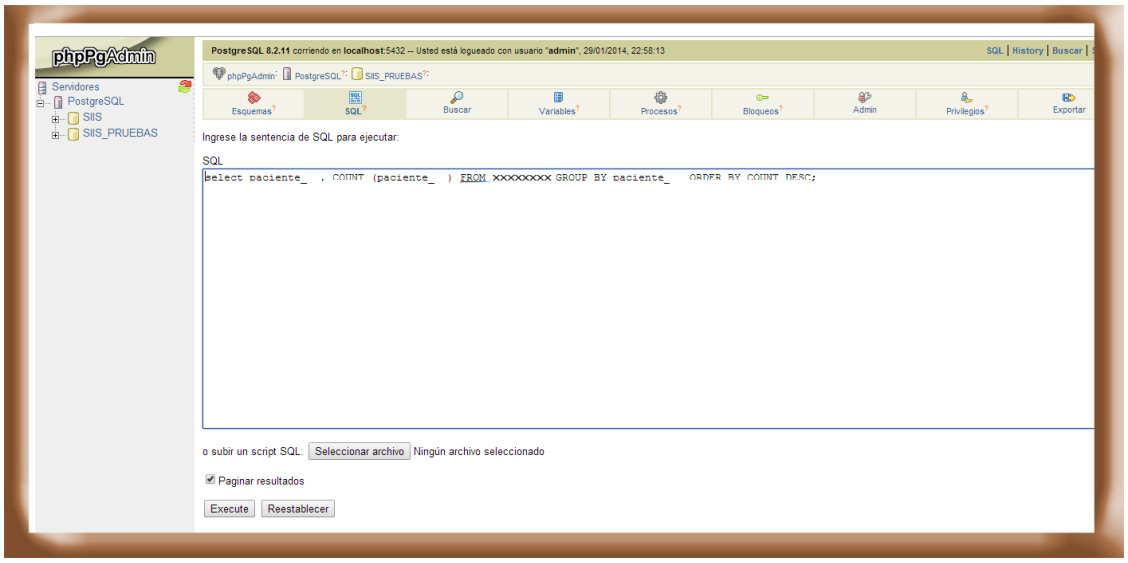


Figura 13. Resultado Consulta

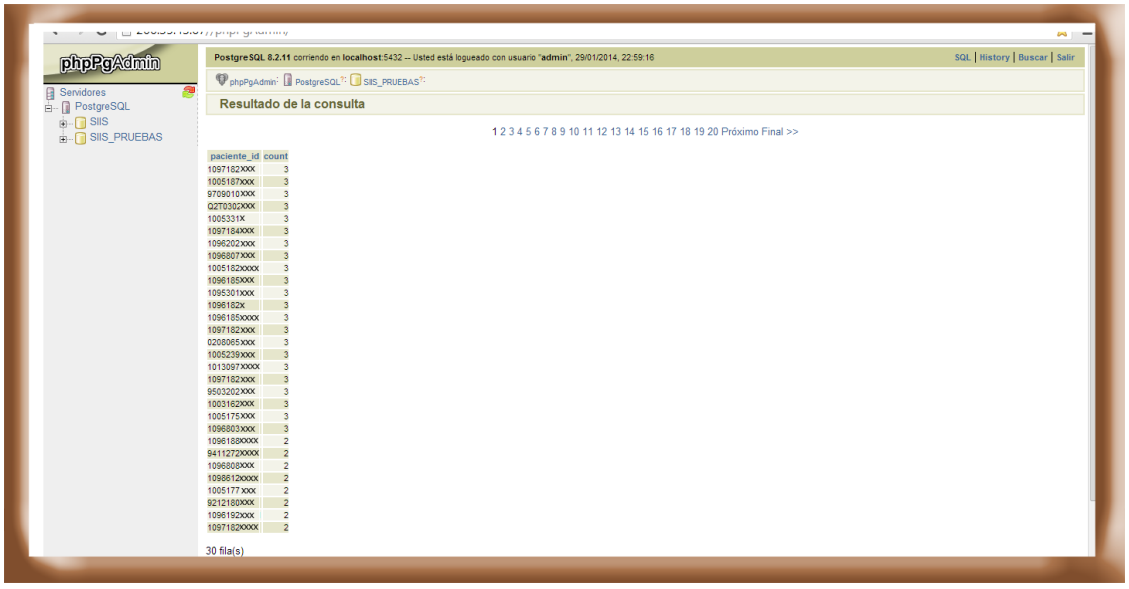
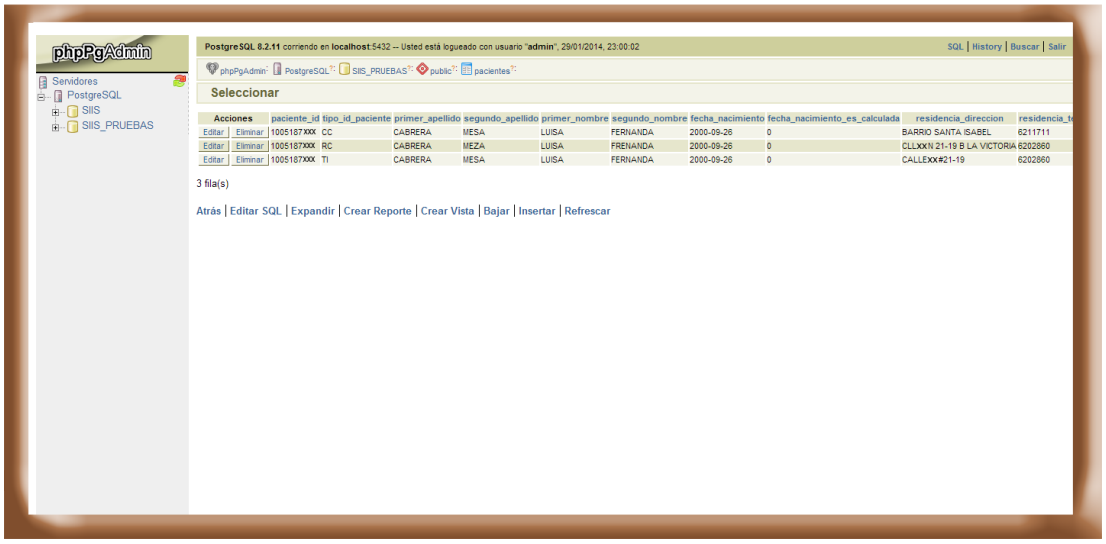


Figura 14. Visualización Duplicado



CONSULTAS CAMPOS NULOS

Objetivo

Verificar la Integridad de los datos

Figura 15. Tabla terxxxxx

Realización de consulta

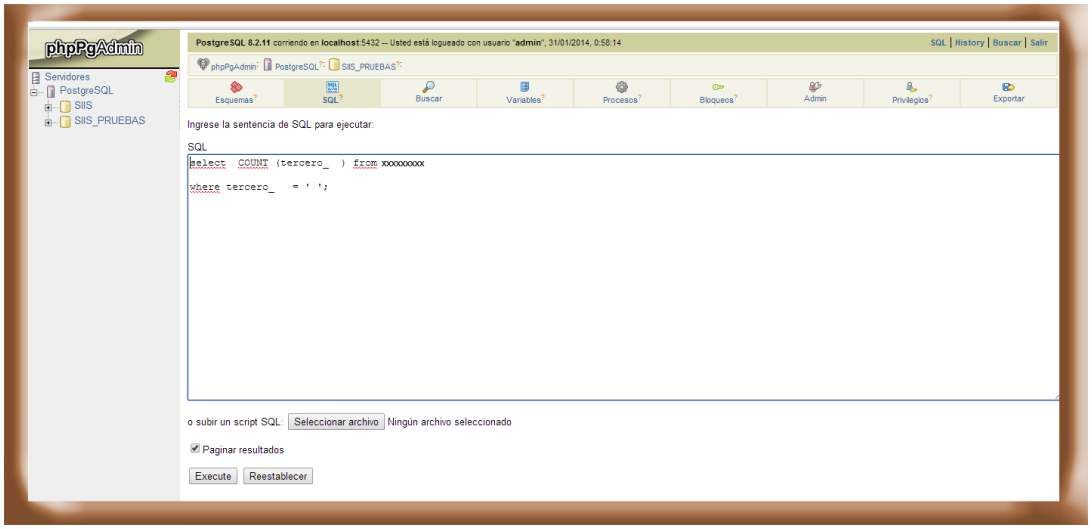


Figura 16. Resultado Consulta

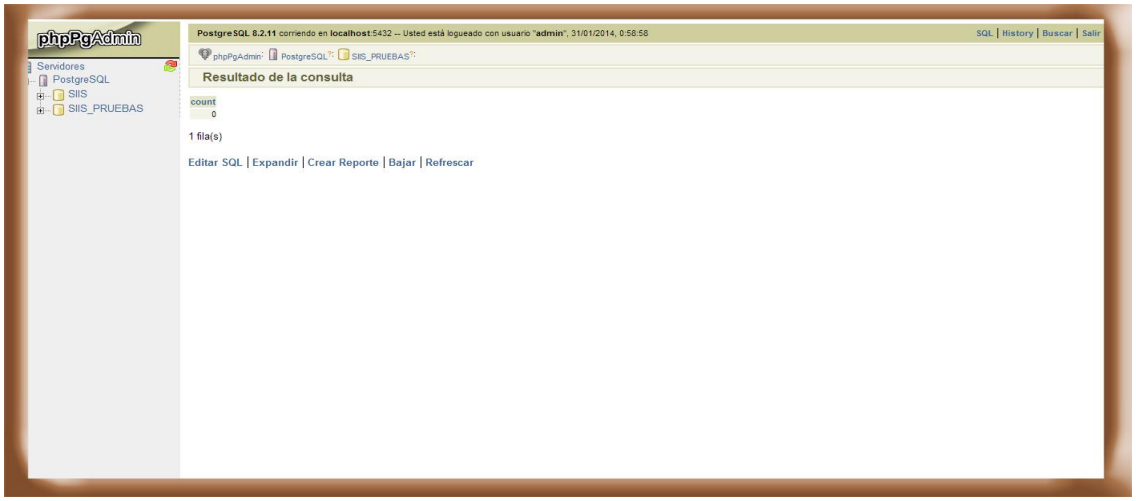


Figura 17. Tabla **os_xxxxxxx**

Realización Consulta

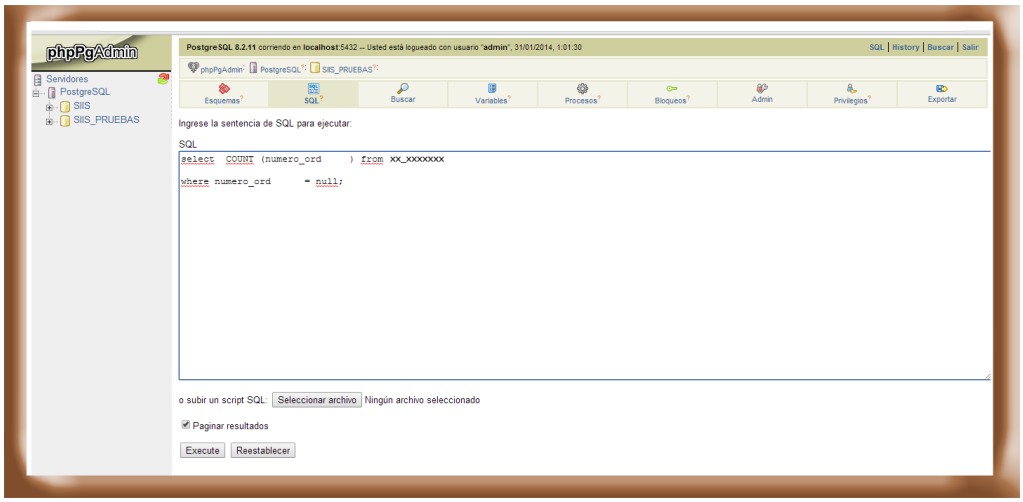


Figura 18. Resultado Consulta

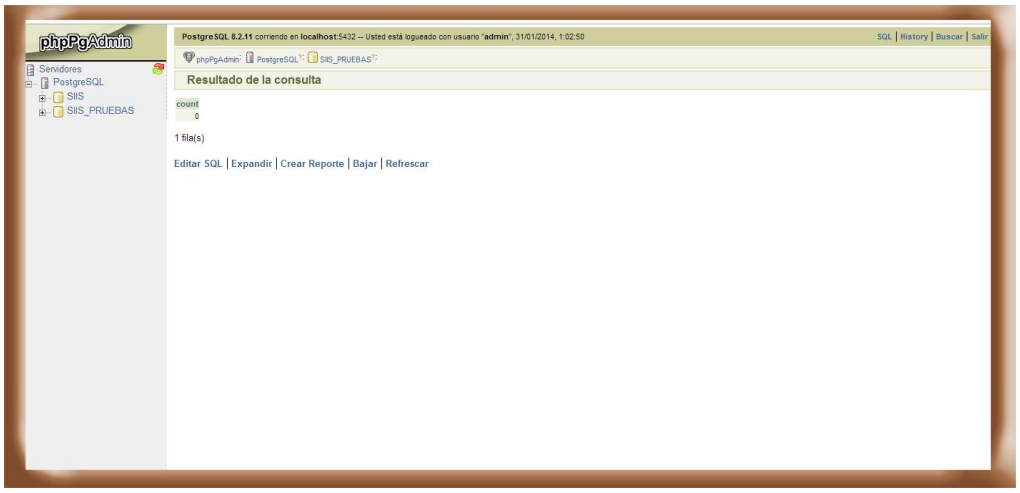


Figura 19. Tabla paxxxxxx

Realización consulta

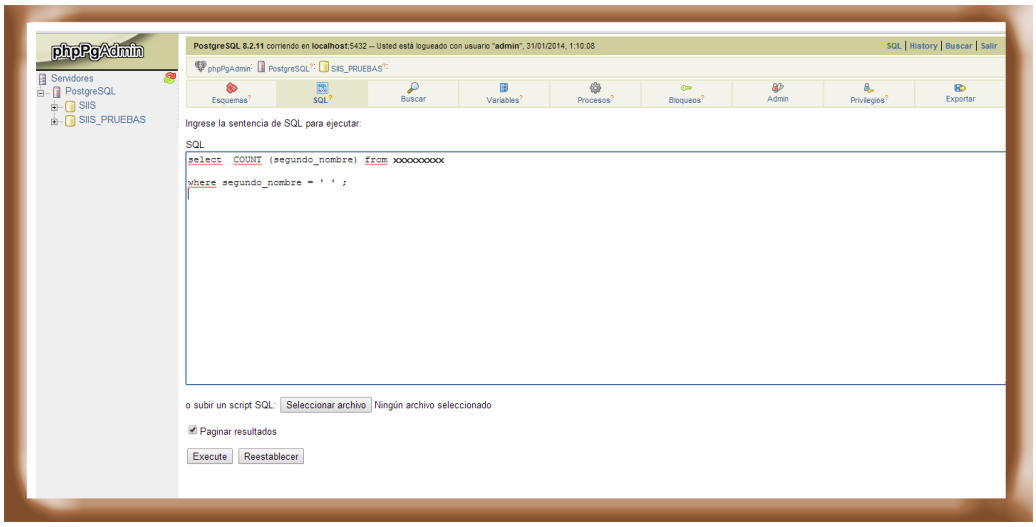


Figura 20. Resultado Consulta

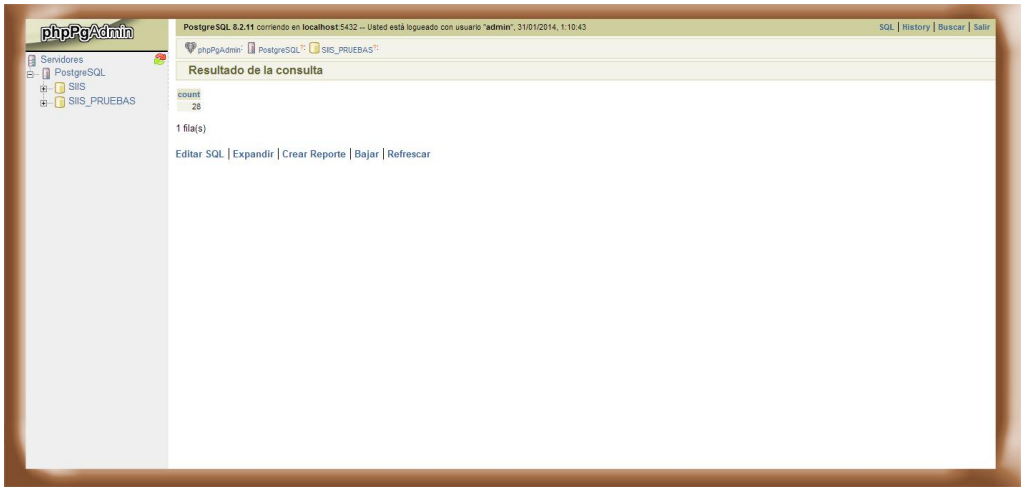


Figura 21. Visualización del estado Nulo del atributo segundo_nombre

VERIFICAR CAMPOS TIPO FECHA (OPERADOR BETWEEN)

Objetivo

Realización de consultas para determinar límites correctos
Verificar integridad de los datos

Figura 22. Tabla terxxxxx

Realización de Consulta

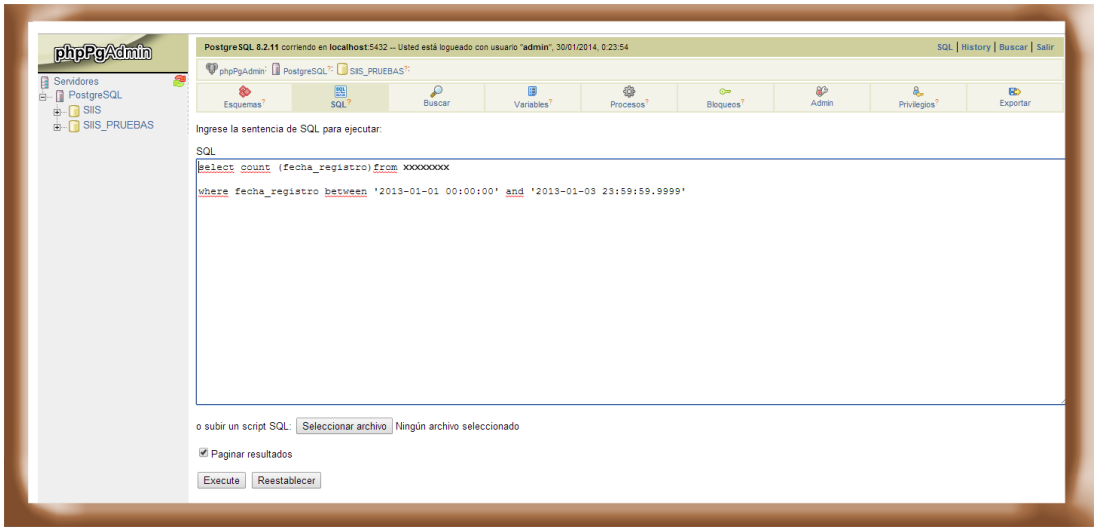


Figura 23. Resultado consulta

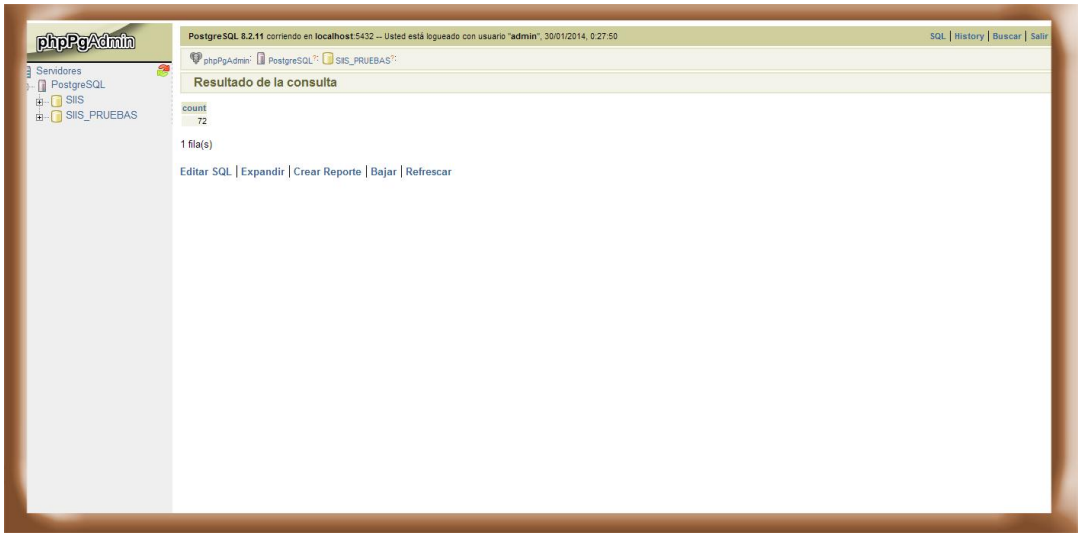


Figura 24. Visualización campos fecha_registo

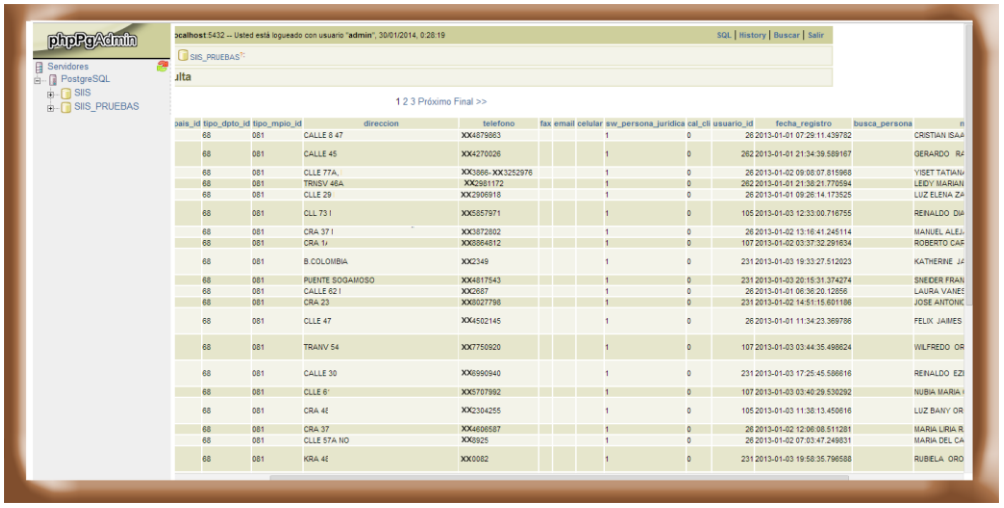


Figura 25. Tabla os_xxxxxxx

Realización Consulta

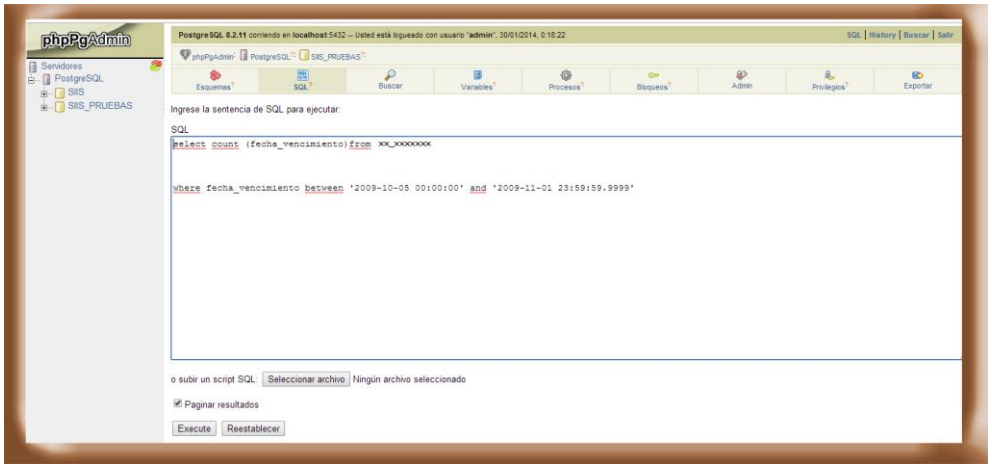


Figura 26. Resultado Consulta

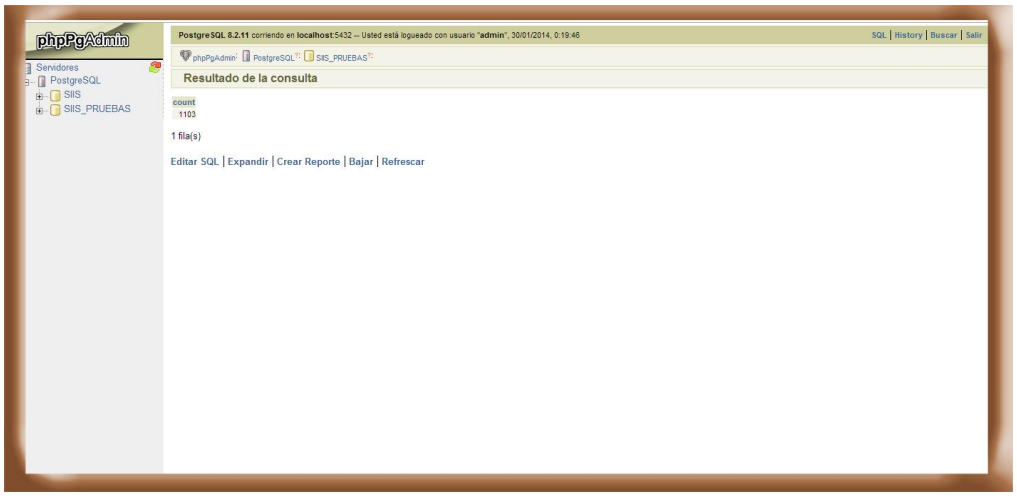
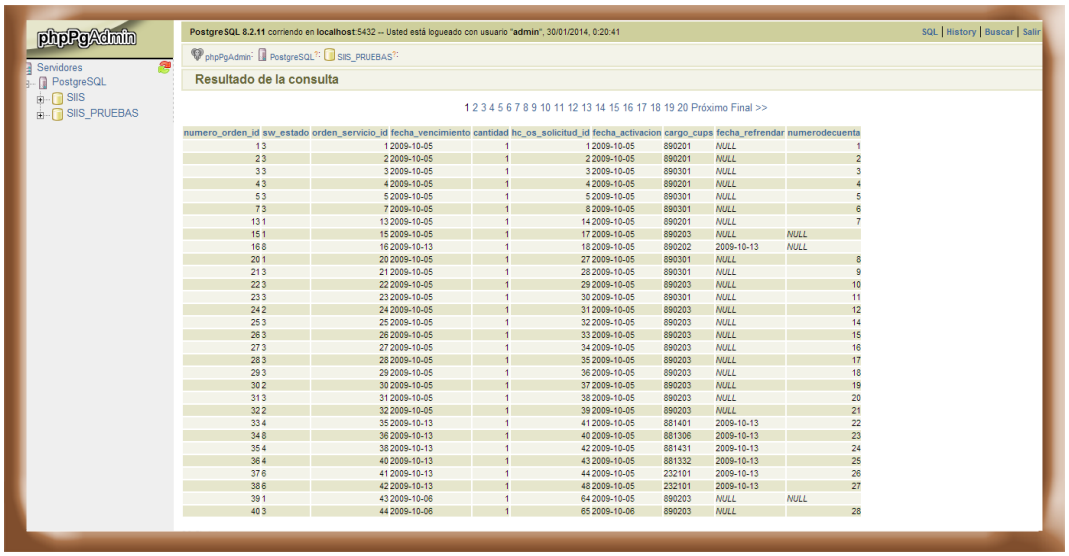


Figura 27. Visualización campo **fecha_vencimiento**



numero_orden_id	sw_estado	orden_servicio_id	fecha_vencimiento	cantidad	hc_os_solicitud_id	fecha_activacion	cargo_cups	fecha_refrendar	numerodecuenta
1	3	1	2009-10-05	1	1	2009-10-05	890201	NULL	1
2	3	2	2009-10-05	1	2	2009-10-05	890201	NULL	2
3	3	3	2009-10-05	1	3	2009-10-05	890301	NULL	3
4	3	4	2009-10-05	1	4	2009-10-05	890201	NULL	4
5	3	5	2009-10-05	1	5	2009-10-05	890301	NULL	5
7	3	7	2009-10-05	1	8	2009-10-05	890301	NULL	6
13	1	13	2009-10-05	1	14	2009-10-05	890201	NULL	7
15	1	15	2009-10-05	1	17	2009-10-05	890203	NULL	NULL
16	8	16	2009-10-13	1	18	2009-10-05	890202	2009-10-13	NULL
20	1	20	2009-10-05	1	27	2009-10-05	890301	NULL	8
21	3	21	2009-10-05	1	28	2009-10-05	890301	NULL	9
22	3	22	2009-10-05	1	29	2009-10-05	890203	NULL	10
23	3	23	2009-10-05	1	30	2009-10-05	890301	NULL	11
24	2	24	2009-10-05	1	31	2009-10-05	890203	NULL	12
25	3	25	2009-10-05	1	32	2009-10-05	890203	NULL	14
26	3	26	2009-10-05	1	33	2009-10-05	890203	NULL	15
27	3	27	2009-10-05	1	34	2009-10-05	890203	NULL	16
28	3	28	2009-10-05	1	35	2009-10-05	890203	NULL	17
29	3	29	2009-10-05	1	36	2009-10-05	890203	NULL	18
30	2	30	2009-10-05	1	37	2009-10-05	890203	NULL	19
31	3	31	2009-10-05	1	38	2009-10-05	890203	NULL	20
32	2	32	2009-10-05	1	39	2009-10-05	890203	NULL	21
33	4	35	2009-10-13	1	41	2009-10-05	881401	2009-10-13	22
34	8	36	2009-10-13	1	40	2009-10-05	881306	2009-10-13	23
35	4	38	2009-10-13	1	42	2009-10-05	881431	2009-10-13	24
36	4	40	2009-10-13	1	43	2009-10-05	881332	2009-10-13	25
37	6	41	2009-10-13	1	44	2009-10-05	232101	2009-10-13	26
38	6	42	2009-10-13	1	48	2009-10-05	232101	2009-10-13	27
39	1	43	2009-10-06	1	64	2009-10-05	890203	NULL	NULL
40	3	44	2009-10-06	1	65	2009-10-06	890203	NULL	28

Anexo Ñ. Formato de Verificación Seguridad Física

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

FORMATO DE VERIFICACION

ENTIDAD: CLINICA SAN JOSE S.A.S. PT. No. SF001
Área: Seguridad Física

Elaboró: H.M.P. Fecha: 26-09-2013
Revisó: M.R.S.R. Fecha: 30-09-2013
Aplicó: H.M.P. Fecha: 21-10-2013

Objetivo: Verificación de la medidas de seguridad física

ÍTEM	ASPECTO	EXISTE		ESTADO			R/PT
		SI	NO	E	R	M	
1.	Aire acondicionado (Sistema de refrigeración)	X		x			EF001
2.	Extintores	X		x			EF002
3.	Conexión eléctrica	X			x		EF003
4.	Conexión de datos	X			x		EF004
5.	Alarma contra incendios		X				
6.	Detector de Humo		X				
7.	Salidas de emergencia	X		x			EF005
8.	Cámaras de vigilancia interior	X				x	EF006
9.	Cámaras de vigilancia exterior		X				
10.	Recolectores de basura (material incombustible)	X		x			EF007
11.	Sistema corriente alterna	X		x			EF009
12.	Vigilancia Privada	X					
13.	Polo a tierra	X		x			EF008
14.	Cableado de datos independiente		X				
15.	Medidas de seguridad física de las copias de respaldo		X				
16.	Plano de Red		X				
17.	Inventario de Equipos	X		x			IE001
18.	Plan de contingencia		X				
19.	Pararrayos		X				
20.	Bitácoras de procedimientos operativos		X				
21.	Medidor de temperatura del Rack	X		x			EF010
22.	Calidad del cableado de Red	X		x			EF011

23.	Cableado en Categoría 6		X				

H.M.P.: Henry Marulanda Padilla – Estudiante de Pasantía
M.R.S.R.: Magreth Rossio Sanguino Reyes – Director Proyecto
SF001: Formato de verificación de las medidas de seguridad física
E: Excelente
R: Regular
M: Malo
R/PT: Referenciación de los Papeles de trabajo
EF001-EF002-EF003-EF004-EF005-EF006-EF007-EF008-EF009-EF010-EF011: Evidencias Fotográficas
IE001: Inventario de equipos de cómputo

VERIFICADO POR

Henry Marulanda P.

HENRY MARULANDA PADILLA
Estudiante de Pasantía

SUPERVISADO POR

NICOLÁS DE LA TORRE VILLARREAL
Coordinador de Procesos

Evidencias para el Formato de Verificación Seguridad Física PT. No. SF001

Foto EF001. Aire Acondicionado

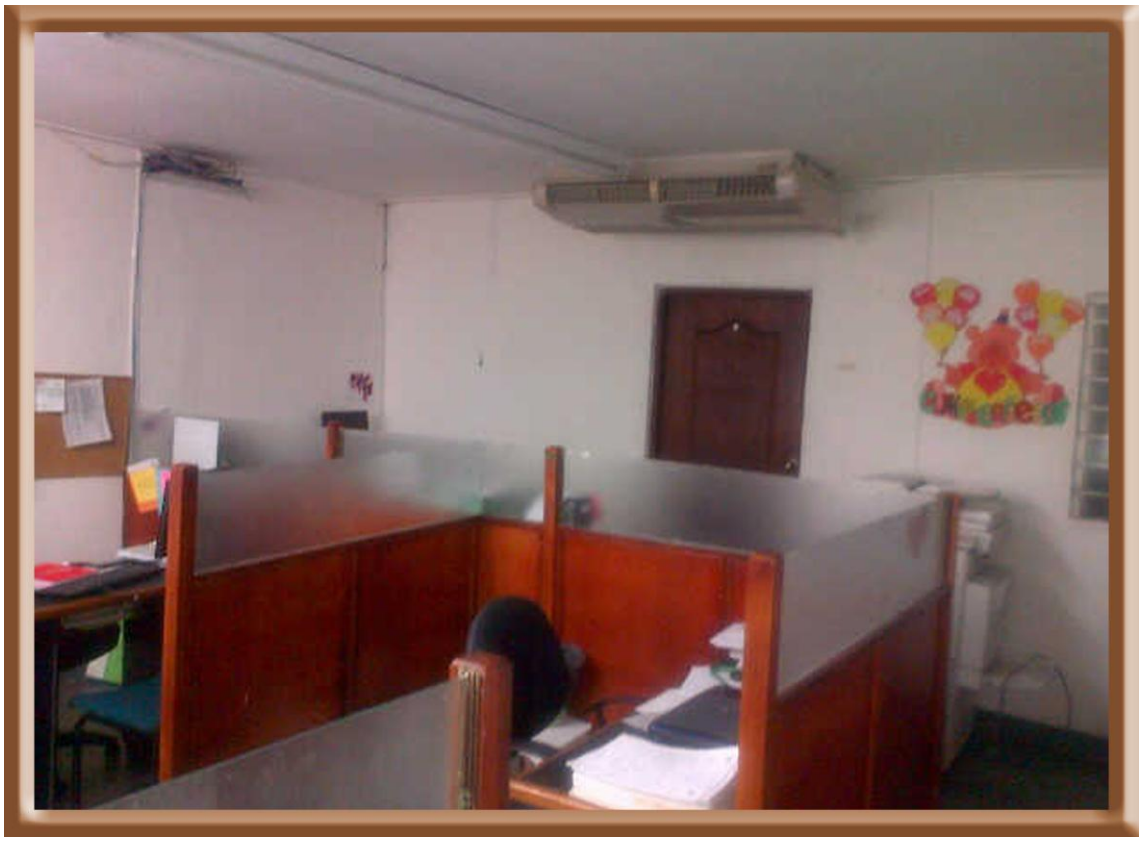


Foto EF002: Extintor

Foto <u>EF003</u>: Conexión Eléctrica

Foto EF004: Conexión de Datos

Foto EF005: Salidas de Emergencias

Foto EF006: Cámaras de vigilancia internas

Foto EF007: Recolector de Basura

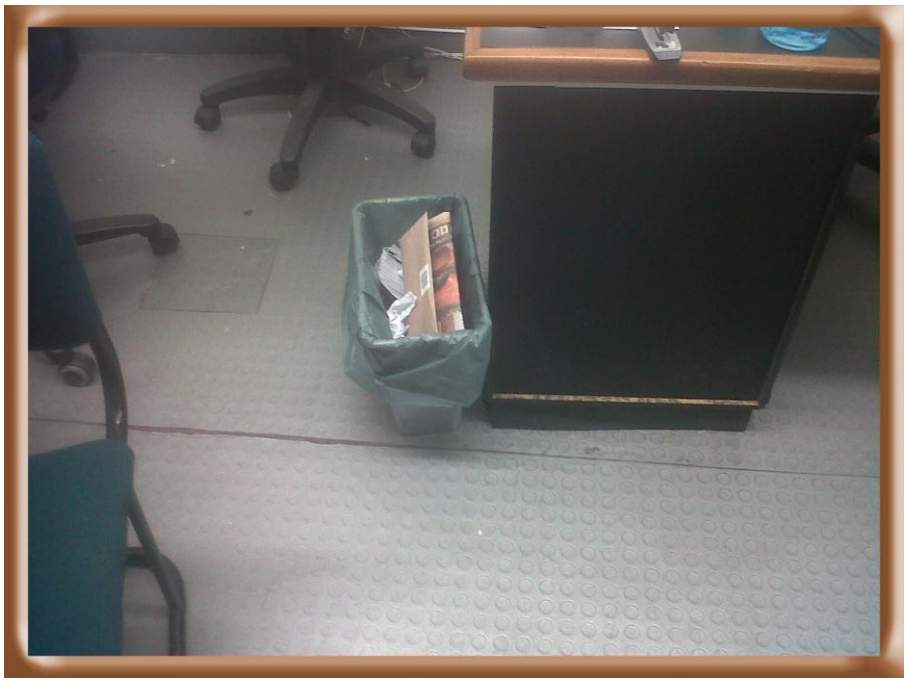
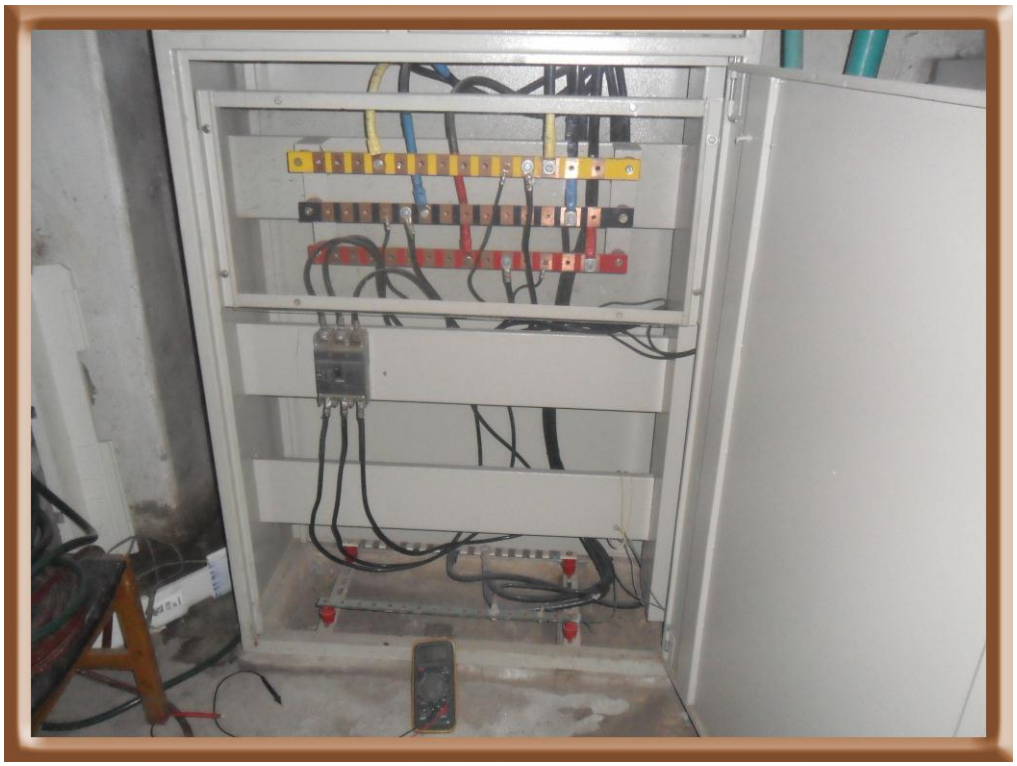


Foto EF009: Sistemas de Corriente Alterna

Foto EF008: Polo a Tierra



Inventario Equipos IE001

CLINICA SAN JOSE S.A.S

INVENTARIO DE SISTEMAS

PT No. IE001

DEPARTAMENTO: Centro Ambulatorio

N. INVENTARIO	DESCRIPCION	REFERENCIA	MARCA	AREA
2273	Teclado	Kb-0316	HP	Recep Cent Ambulatorio
2275	CPU	Xl808av#219	HP	Recep Cent Ambulatorio
2276	Monitor	Hplv1911	HP	Recep Cent Ambulatorio
2277	Mouse	M-s0005-0	HP	Recep Cent Ambulatorio
1748	Impresora	Photo smart c4280	HP	Recep Cent Ambulatorio
1599	Teclado	K639	GENIUS	Fact Cent Ambulatirio
126	CPU	Clon	CLON	Fact Cent Ambulatirio
93	Monitor	Hsg 1044	QBEX	Fact Cent Ambulatirio
2279	Mouse	Xscroll	GENIUS	Fact Cent Ambulatirio
1340	Impresora	Laserjet P2055dn	HP	Fact Cent Ambulatirio
2278	Scaner	scanjet professional 1000	HP	Fact Cent Ambulatirio
2519	Teclado	BAUVTOBHH1A0NL	HP	Vacunacion
105	CPU	Kronos 5810290	QBEX	Vacunacion
104	Monitor	Hsg 1044	QBEX	Vacunacion
2282	Mouse	1f3f72d	QBEX	Vacunacion
782	Teclado	K9852	Delux	Consultorio 2
2283	CPU	Kronos 5810290	QBEX	Consultorio 2
89	Monitor	Hsg 1044	QBEX	Consultorio 2
115	Mouse	1f3f72d	QBEX	Consultorio 2
119	Teclado	KB-1000	OMEGA	Consultorio 3

109	CPU	Kronos 5810290	QBEX	Consultorio 3
117	Monitor	Hsg 1044	QBEX	Consultorio 3
2280	Mouse	Net scroll 120	GENIUS	Consultorio 3
1788	Teclado	Kb-06xe	QBEX	Fisioterapia
145	CPU	CLON	CLON	Fisioterapia
445	Monitor	T71w	BENQ	Fisioterapia
2281	Mouse	Gm-03022p	GENIUS	Fisioterapia
DEPARTAMENTO: Mantenimiento				
2284	Teclado	K639	GENIUS	Mantenimiento
2237	CPU	CLON	CLON	Mantenimiento
103	Monitor	Hsg 1044	QBEX	Mantenimiento
2285	Mouse	Net scroll 120	GENIUS	Mantenimiento
DEPARTAMENTO: Cuarto Piso UCI				
2138	Teclado	Kb-0316	HP	Equipo 1
2137	CPU	MXL2181JRP	HP	Equipo 1
2136	Monitor	LV1911	HP	Equipo 1
2139	Mouse	S-0005O	HP	Equipo 1
2142	Teclado	KB-0316	HP	Equipo 2
2141	CPU	MXL2180C27	HP	Equipo 2
2140	Monitor	LV1911	HP	Equipo 2
2143	Mouse	60053-002	HP	Equipo 2
DEPARTAMENTO: Tercer Piso				
2286	Teclado	KB-06XE	GENIUS	Enfermeria Equipo 1
1306	CPU	CLON	CLON	Enfermeria Equipo 1
2172	Monitor	T71W	DENQ	Enfermeria Equipo 1
2287	Mouse	Gm-03022p	GENIUS	Enfermeria Equipo 1
2175	Teclado	KB-0316	HP	Enfermeria Equipo 2
2288	CPU	COMPAQ 400 PRO SFF	HP	Enfermeria Equipo 2
2289	Monitor	LV1911	HP	Enfermeria Equipo 2
2176	Mouse	600553-002	HP	Enfermeria Equipo 2
1412	IMPRESORA	Laserjet P2055dn	HP	Enfermeria Equipo 2
2587	Teclado	Kb-110x	GENIUS	Facturacion
2198	CPU	Kronos 5810290	QBEX	Facturacion
2290	Monitor	Hsg 1044	QBEX	Facturacion

1016	Mouse	537750-001	GENIUS	Facturacion
DEPARTAMENTO: Segundo Piso				
1472	Teclado	KB-1000	OMEGA	Fact Cirugia
446	CPU	CLON	CLON	Fact Cirugia
2291	Monitor	Hsg 1044	QBEX	Fact Cirugia
1854	Mouse		Next	Fact Cirugia
2292	Impresora	F7bf031569	EPSON	Fact Cirugia
1474	Impresora	Laserjet P2055dn	HP	Fact Cirugia
128	Teclado	KB-1000	OMEGA	Enfermeros
2293	CPU	CLON	CLON	Enfermeros
118	Monitor	Hsg 1044	QBEX	Enfermeros
2485	Mouse	JW-cskm02	JAWAN	Enfermeros
1074	Computador Portatil	Presario C700	COMPAQ	Cirugia
2294	Computador Portatil	Aspire 4739	.ACER	Cirugia
2295	Teclado	K639	GENIUS	Cirugia
1335	CPU	Blue Code	CLON	Cirugia
1533	Monitor	W1943SG-PF	LG	Cirugia
2225	Mouse	216125e	QBEX	Cirugia
DEPARTAMENTO: Primer Piso				
2236	Teclado	KU-0138	GENIUS	Fact Urgencias
1172	CPU	5050MT	COMPAQ	Fact Urgencias
1171	Monitor	HP Le1901W	HP	Fact Urgencias
1174	Mouse	537750-001	GENIUS	Fact Urgencias
2296	Impresora	Lase Jet pro 400 MPF	HP	Fact Urgencias
2298	Teclado	K639	GENIUS	Consultorio 1
2300	CPU	TWIN 36102901	QBEX	Consultorio 1
2297	Monitor	IH182APB	QBEX	Consultorio 1
2299	Mouse	GM-03022P	GENIUS	Consultorio 1
2301	Teclado	SK-8115	DELL	Consultorio 2
2303	CPU	KRONOS 5810290	QBEX	Consultorio 2
125	Monitor	T71W	BENQ	Consultorio 2
2302	Mouse	GM-03022P	GENIUS	Consultorio 2
2304	Estabilizador	IEN-AVER1006	NEW	Consultorio 2

2307	Teclado	K639	GENIUS	Triage
890	CPU	KRONOS 5810290	QBEX	Triage
2306	Monitor	IH182APB	QBEX	Triage
2305	Mouse	Net scroll 120	GENIUS	Triage
2106	Computador Portatil	3c275176w	TOSHIBA	Triage
1921	Teclado	Sk-8110	DELL	Estcn enfermeria Eq1
2310	CPU	KRONOS 5810290	QBEX	Estcn enfermeria Eq1
55	Monitor	IH182APB	QBEX	Estcn enfermeria Eq1
2309	Mouse	GM-03022P	GENIUS	Estcn enfermeria Eq1
2308	Impresora	Hp Laser Jet P2035n	HP	Estcn enfermeria Eq1
2311	Estabilizador	Propc	NIOMAR	Estcn enfermeria Eq1
2314	Teclado	K639	GENIUS	Estcn enfermeria Eq2
97	CPU	KRONOS 5810290	QBEX	Estcn enfermeria Eq2
2312	Monitor	Hsg 1044	QBEX	Estcn enfermeria Eq2
2313	Mouse	GM-03022P	GENIUS	Estcn enfermeria Eq2
1772	Teclado	K639	GENIUS	Rayos X
435	CPU	CLON	CLON	Rayos X
1117	Monitor	W1934SI	LG	Rayos X
2315	Mouse	GM-03022P	GENIUS	Rayos X
2316	Impresora	GK420T	ZEBRA	Rayos X
DEPARTAMENTO: Farmacia				
2319	Teclado	539130-161	HP	Equipo 1
2317	CPU	MXL202020v	HP	Equipo 1
2318	Monitor	S1933	HP	Equipo 1
2320	Mouse	265966-011	HP	Equipo 1
2321	Teclado	Kb-0316	HP	Equipo 2
2323	CPU	MXL218146L	HP	Equipo 2
151	Monitor	913FW	AOC	Equipo 2
2566	Mouse	jw- cskm 02	JAWAN	Equipo 2
DEPARTAMENTO: Apoyo Diagnostico				
2324	Teclado	Kb-0316	HP	Apoyo Diagnostico
2327	CPU	MXL218146L	HP	Apoyo Diagnostico
2325	Monitor	Lv1911	HP	Apoyo Diagnostico
2326	Mouse	537748-001	HP	Apoyo Diagnostico

1349	Impresora	Laserjet P2055dn	HP	Apoyo Diagnostico
1904	Scaner	scanjet professional 1000	HP	Apoyo Diagnostico
DEPARTAMENTO: Laboratorio				
2328	Teclado	164.960.304.851	GENIUS	Laboratorio
422	CPU	CLON	DELUX	Laboratorio
779	Monitor	HW173A	QBEX	Laboratorio
1107	Mouse			Laboratorio
DEPARTAMENTO: Administracion				
2330	Teclado	Kb-0316	HP	Archivo
2332	CPU	MXL218146L	HP	Archivo
2331	Monitor	Lv1911	HP	Archivo
2329	Mouse	60053-002	HP	Archivo
2333	Estabilizador		NEW LINE	Archivo
2334	CPU	CLON	CLON	Secrt Auxiliar
434	Monitor	PL-19b	PROVIEW	Secrt Auxiliar
2336	Mouse	GM-03022P	GENIUS	Secrt Auxiliar
2337	Teclado	539130-161	HP	Fact. Y Auditoria
2340	CPU	MXL1151D18	HP	Fact. Y Auditoria
2339	Monitor	S2021	CONPAQ	Fact. Y Auditoria
2338	Mouse	26598-011	HP	Fact. Y Auditoria
2341	Teclado	K639	GENIUS	Glosas
1601	CPU	CLON	CLON	Glosas
1598	Monitor	E1920NX	SANSUNG	Glosas
2342	Mouse	60053-003	HP	Glosas
2343	Teclado	Kb-0316	HP	Auditoria Coomeva
2345	CPU	MXL1151D18	HP	Auditoria Coomeva
159	Monitor	716Sw	AOC	Auditoria Coomeva
2344	Mouse	Net scroll 120	GENIUS	Auditoria Coomeva
1305	Teclado	K639	GENIUS	Aux Administrativa
2402	CPU	CLON	CLON	Aux Administrativa
2347	Monitor	Lv1911	HP	Aux Administrativa
2346	Mouse	Net scroll 120	GENIUS	Aux Administrativa
2350	CPU	MXL202020G	HP	secretaria

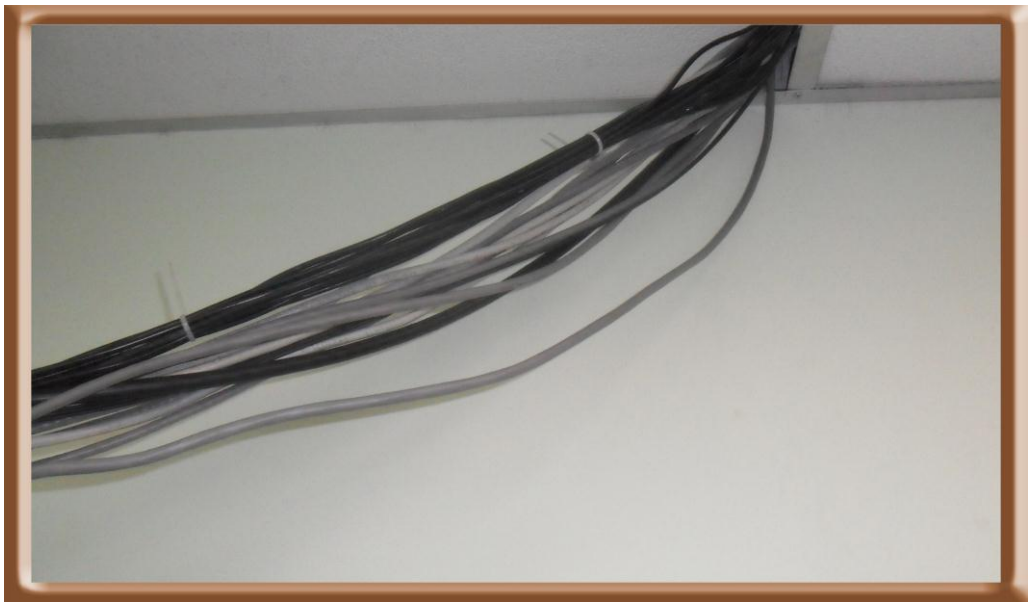
2349	Monitor	LV1911	HP	secretaria
2348	Mouse	265966-011	HP	secretaria
1024	Teclado	KB-1000	OMEGA	secretaria
1359	Computador Portatil	ASPIRE 5338	.Acer	Jefe de Sistemas
2351	Mouse	Net scroll 100x	GENIUS	Jefe de Sistemas
2352	Teclado	539130-161	HP	Envios
2354	CPU	MXL1151D00	HP	Envios
1631	Monitor	WM767A	COMPAQ	Envios
2353	Mouse	265966-011	HP	Envios
2356	Teclado	539130-161	HP	Director Administrativo
2357	CPU	MXL202020L	HP	Director Administrativo
2358	Monitor	XJ311A	HP	Director Administrativo
2355	Mouse	265966-011	HP	Director Administrativo
1173	Teclado	505130-011	HP	Gerente de Servicios
1634	CPU	MXL1011R6C	HP	Gerente de Servicios
1628	Monitor	S2021	COMPAQ	Gerente de Servicios
2359	Mouse	265986-011	HP	Gerente de Servicios
1629	Teclado	KB-1000	OMEGA	Salud Ocupacional 1
102	CPU	CLON	CLON	Salud Ocupacional 1
1212	Monitor	E170Sc	DELL	Salud Ocupacional 1
2360	Mouse	GM-03022P	GENIUS	Salud Ocupacional 1
2361	Estabilizador	Propc	NIOMAR	Salud Ocupacional 1
1301	Teclado	L-358c	QBEX	Salud Ocupacional 2
1211	CPU	CLON	CLON	Salud Ocupacional 2
2363	Monitor	E1942c-BN	LG	Salud Ocupacional 2
2362	Mouse	GM-03022P	GENIUS	Salud Ocupacional 2
2335	Teclado	53130-161X	HP	Aux Contable
2365	CPU	MXL1131BZ9	HP	Aux Contable
2366	Monitor	S2021	COMPAQ	Aux Contable
2364	Mouse	265986-011	HP	Aux Contable
2368	Teclado	KB-1000	OMEGA	Aux Tesoreria
2369	CPU	MXL2020217	HP	Aux Tesoreria

2370	Monitor	S1933	HP	Aux Tesoreria
2367	Mouse	265986-011	HP	Aux Tesoreria
2372	Teclado	CSS-720	PC SMART	Aux Cartera
2373	CPU		PC SMART	Aux Cartera
67	Monitor	HW173A	QBEX	Aux Cartera
2371	Mouse	CSS-720	PC SMART	Aux Cartera
2375	Teclado	K639	GENIUS	Contadora
149	CPU	CLON	CLON	Contadora
1308	Monitor	S19A300B	SANSUNG	Contadora
1663	Mouse	Net scroll 120	GENIUS	Contadora
2374	Impresora	LX-300+II	EPSON	Contadora
1720	Teclado	539130-161	HP	Gerencia
1723	CPU	MXL1611RSQ	HP	Gerencia
1719	Monitor	S2021	COMPAQ	Gerencia
1721	Mouse	265986-011	HP	Gerencia
DEPARTAMENTO: Avanzar				
415	Computador Portatil	ASPIRE 5338	.Acer	Odontologia Eqp 1
1317	Computador Portatil	ASPIRE 5338	.Acer	Odontologia Eqp 2
2376	Mouse	Xscroll	GENIUS	Odontologia Eqp 2
DEPARTAMENTO: Sistemas				
2221	Servidor	Power edge 2600	DELL	Sistemas
2222	Servidor	Power edge 2900	DELL	Sistemas
1030	Servidor	Power edge 2600	DELL	Sistemas
1046	Servidor	Power edge 1900	DELL	Sistemas
2223	UPS	Electra	QBEX	Sistemas
1013	UPS	Ecoserver ups	QUEST	Sistemas
2231	Rack	Super stack	3COM	Sistemas
2232	Dvr	tv-7216	Network dvr	Sistemas
76	Monitor	Hw 173a	QBEX	Sistemas
38	Monitor	Flatron ez t730sh	LG	Sistemas
1600	Mouse	Zmo 344	GENIUS	Sistemas
1075	Mouse	Um 2018	katec	Sistemas
87	Teclado	Y-UM76A	LOGITECH	Sistemas
144	Teclado	K639	GENIUS	Sistemas

1071	Radio	Pmn 4000d	MOTOROLA	Sistemas
1072	Radio	Pmn 4000d	MOTOROLA	Sistemas

Foto EF010: Medidor de Temperatura del Rack

Foto EF011: Calidad del Cableado de Red



Anexo O. Formato de Verificación Seguridad Lógica

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERÍAS
PLAN DE ESTUDIOS DE INGENIERÍA DE SISTEMAS

EVALUACIÓN MEDIANTE EL ESTÁNDAR ISO 27001 DE LA SEGURIDAD FÍSICA Y LÓGICA DE LA INFRAESTRUCTURA TECNOLÓGICA DE LA CLÍNICA SAN JOSÉ S.A.S DE LA CIUDAD DE BARRANCABERMEJA – SANTANDER.

FORMATO DE VERIFICACION

ENTIDAD: CLINICA SAN JOSE S.A.S. PT. No. SL001
Área: Seguridad Lógica

Elaboró: H.M.P. Fecha: 27-09-2013
Revisó: M.R.S.R. Fecha: 30-09-2013
Aplicó: H.M.P. Fecha: 21-10-2013

Objetivo: Verificación de los mecanismos de Seguridad Lógica

ÍTEM	ASPECTO	EXISTE		R/PT
		SI	NO	
1.	Restricción de acceso al equipo	X		EF012
2.	Software Anti Espía		X	
3.	Software antivirus actualizado	X		EF013
4.	Restricción de acceso a base de datos	X		EF014
5.	Licencias de software	X		EF015
6.	Copias de respaldo	X		EF022
7.	Registro de copias de respaldo	X		BK001
8.	Acuerdos de confidencialidad documentados		X	
9.	Políticas de seguridad de la información		X	
10.	Pólizas contra robo		X	
11.	Pólizas contra incendios		X	
13.	Programas de Recuperación de archivos	X		EF016
14.	Auditorías periódicas a los medios de almacenamiento		X	
15.	Configuración de Proxy	X		EF017

H.M.P.: Henry Marulanda Padilla
M.R.S.R.: Magreth Rossio Sanguino Reyes – Director Proyecto
SL001: Formato de verificación de los mecanismos de Seguridad Lógica
R/PT: Referenciación de los Papeles de trabajo
EF012-EF013-EF014-EF015-EF016-EF017-EF022: Evidencias Fotográficas
BK001: Registro de realización de copias de respaldo

VERIFICADO POR

Henry Marulanda P.

HENRY MARULANDA PADILLA
Estudiante de Pasantía

SUPERVISADO POR

NICOLÁS DE LA TORRE VILLLARREAL
Coordinador de Procesos

Foto <u>EF012</u>: Restricción de Acceso al equipo

Foto <u>EF013</u>: Software Antivirus Actualizado

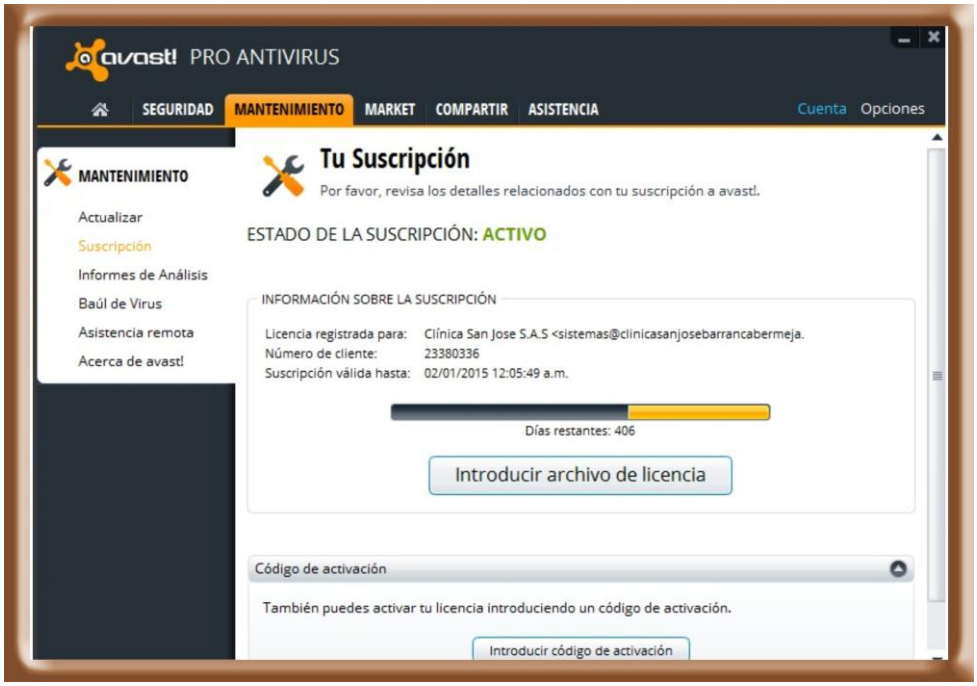


Foto <u>EF014</u>: Restricción de Acceso a Base de Datos

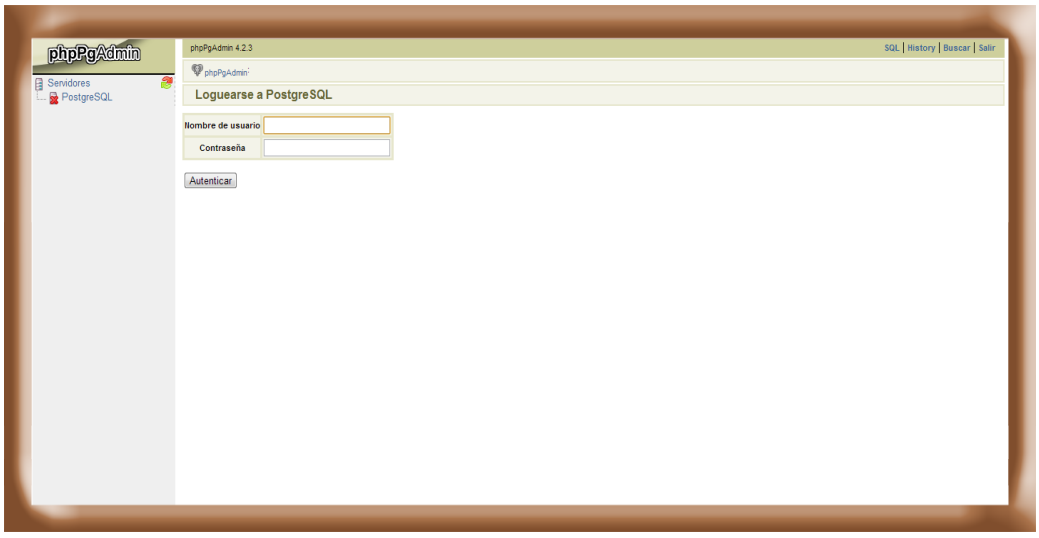


Foto <u>EF015</u>: Licencias de Software

ENTRAR AL SERVIDOR POR MEDIO DE LA HERRAMIENTA PuTTY

PT. No. EF022

Figura 1. Ingreso al PuTTy

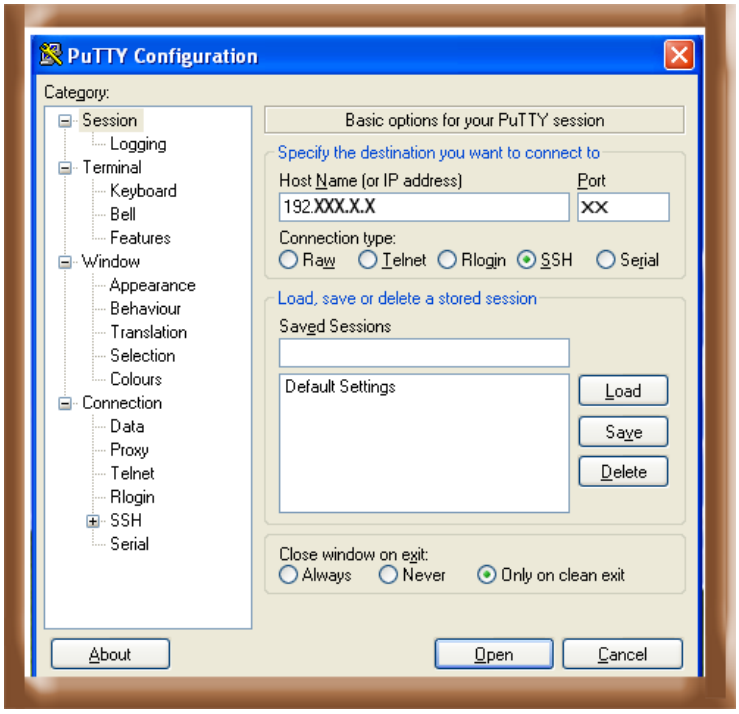


Figura 2. Identificación (Login) en el Servidor

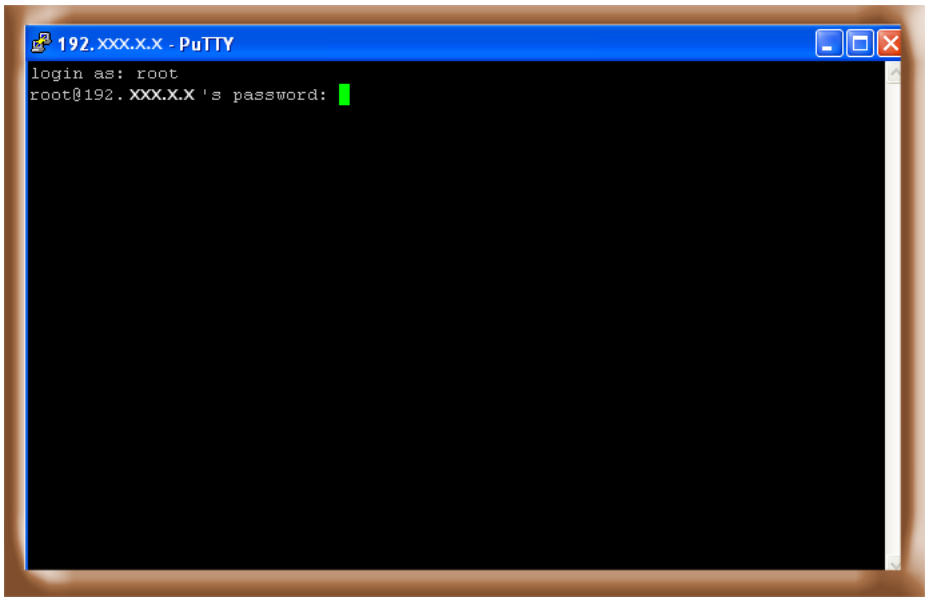


Figura 3. Ruta de Acceso

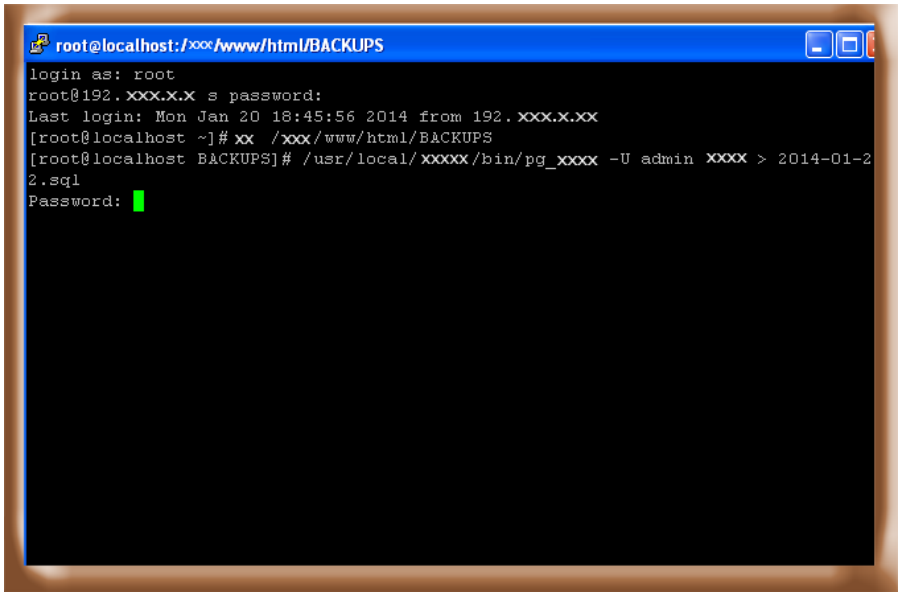


Figura 4. Realización copia de seguridad base de datos con la herramienta winSCP.

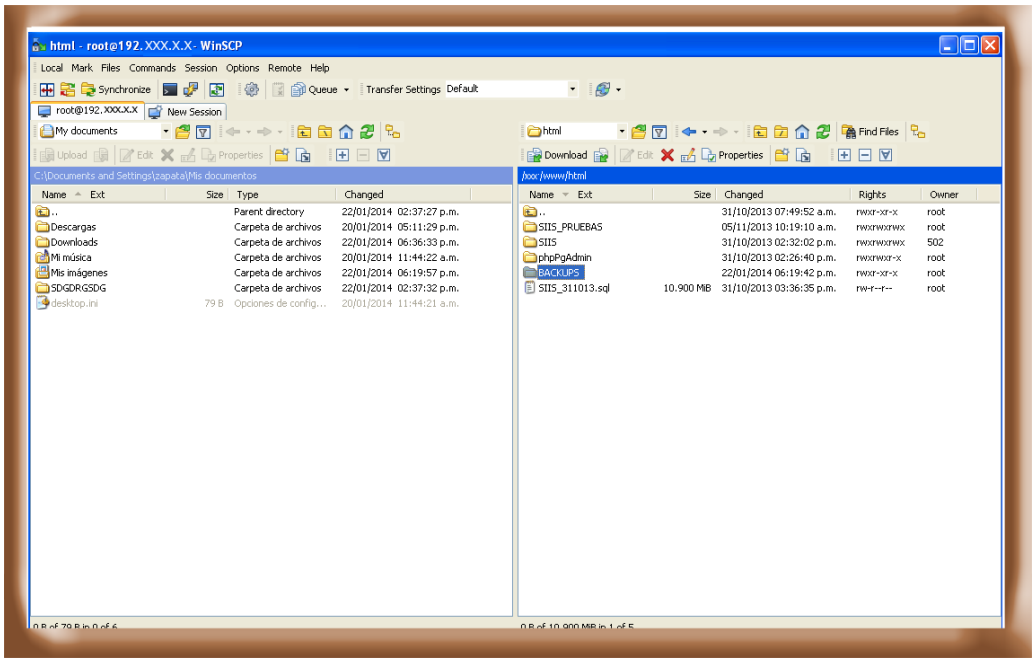
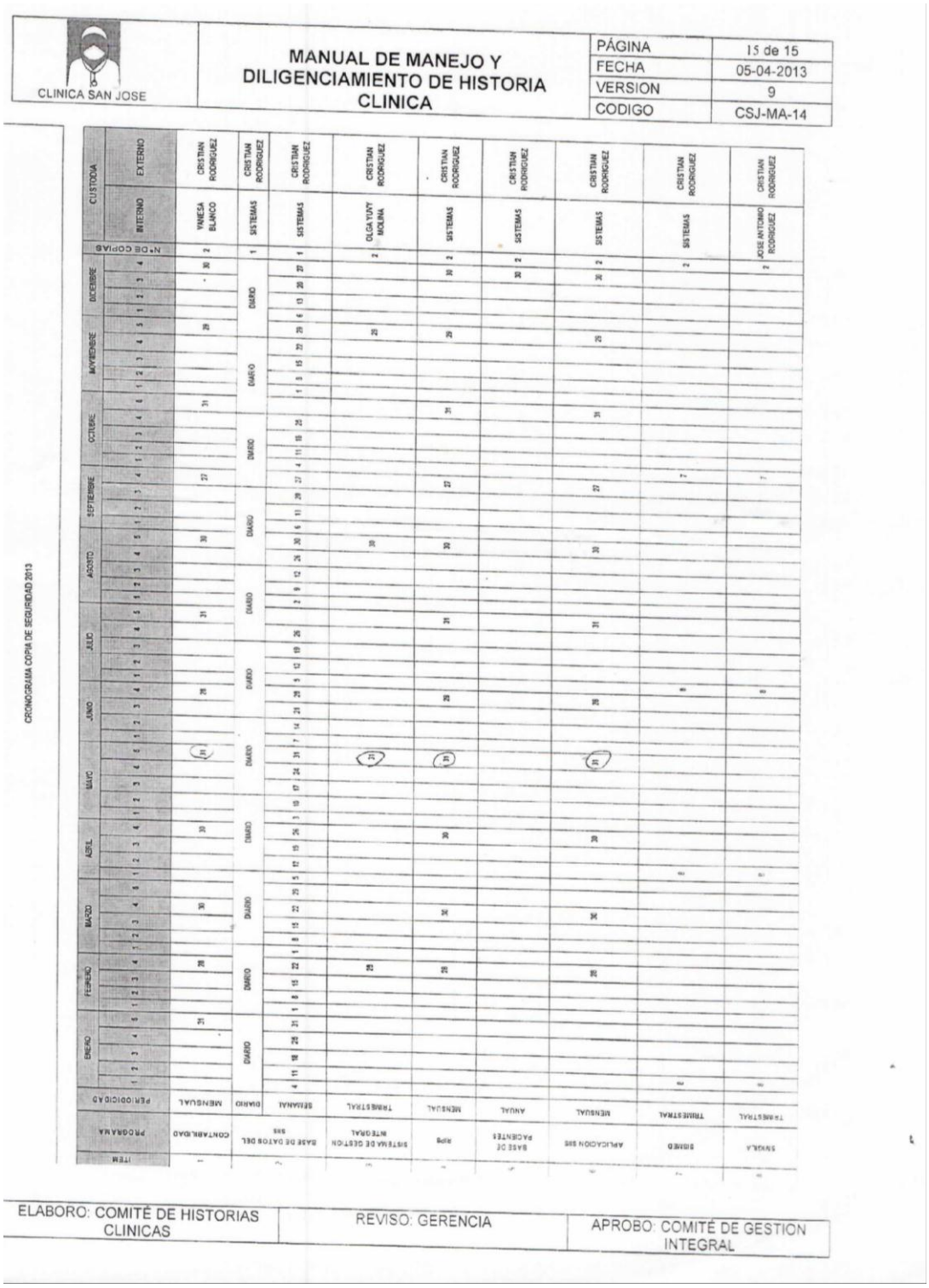


Figura BK001: Registro de Copias de Respaldo



CLINICA SAN JOSE

MANUAL DE MANEJO Y DILIGENCIAMIENTO DE HISTORIA CLINICA

PÁGINA	15 de 15
FECHA	05-04-2013
VERSION	9
CODIGO	CSJ-MA-14

CRONOGRAMA COPIA DE SEGURIDAD 2013

ITEM	PROGRAMA	PERIODICIDAD	CUSTODIA		ENERO	FEBRERO	MARZO	ABRIL	MAYO	JUNIO	JULIO	AGOSTO	SEPTIEMBRE	OCTUBRE	NOVIEMBRE	DICIEMBRE
			INTERNO	EXTERNO												
1	SYNSOLA	TRIMESTRAL	JOSE ANTONIO RODRIGUEZ	CRISTIAN RODRIGUEZ												
2	SIGMED	TRIMESTRAL	SISTEMAS	CRISTIAN RODRIGUEZ												
3	APLICACION SIIS	MENSUAL	SISTEMAS	CRISTIAN RODRIGUEZ												
4	BASE DE PACIENTES	ANUAL	SISTEMAS	CRISTIAN RODRIGUEZ												
5	RIPS	MENSUAL	SISTEMAS	CRISTIAN RODRIGUEZ												
6	SISTEMA DE GESTION INTEGRAL	TRIMESTRAL	OLGA YUVY MOLINA	CRISTIAN RODRIGUEZ												
7	BASE DE DATOS DEL SIIS	SEMANAL	SISTEMAS	CRISTIAN RODRIGUEZ												
8	CONTABILIDAD	DIARIO	SISTEMAS	CRISTIAN RODRIGUEZ												
9		MENSUAL	VANESA BLANCO	CRISTIAN RODRIGUEZ												
			N° DE COPIAS													

ELABORO: COMITÉ DE HISTORIAS CLINICAS | REVISO: GERENCIA | APROBO: COMITÉ DE GESTION INTEGRAL

Foto <u>EF016</u>: Programa de Recuperación de Archivos

Foto EF017: Configuración de Proxy