AUDITORÍA A LA SEGURIDAD INFORMÁTICA DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA E.S.E HOSPITAL SAN FRANCISCO DE GACHETÁ

FRANCISCO JAVIER HILARION NOVOA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CUNDINAMARCA
2017

AUDITORÍA A LA SEGURIDAD INFORMÁTICA DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA E.S.E HOSPITAL SAN FRANCISCO DE GACHETÁ

FRANCISCO JAVIER HILARION NOVOA

ASESOR DE PROYECTO

HERNANDO JOSÉ PEÑA HIDALGO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
CUNDINAMARCA
2017

Nota de aceptación

_____

_____

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Gachetá, _____

DEDICATORIA

A mi familia, a Liz Ortiz y la Universidad Nacional Abierta y a Distancia, por el apoyo brindado en el transcurso de esta especialización.

Francisco Hilarión

AGRADECIMIENTOS

A Dios todo poderoso por la salud, la vida y el conocimiento.

A mi familia por su apoyo y comprensión.

Al cuerpo docente de la Universidad Nacional Abierta y a Distancia UNAD por transmitir sus conocimientos durante este tiempo de formación posgradual.

Al Ingeniero Hernando José Peña por las sugerencias realizadas y por su acompañamiento en el proceso.

Al Ingeniero Francisco Solarte por las sugerencias realizadas y por su acompañamiento en el proceso.

Al Ingeniero Salomón González por las sugerencias realizadas y por su acompañamiento en el proceso.

CONTENIDO

Pág.

ANEXOS

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

TITULO

AUDITORÍA A LA SEGURIDAD INFORMÁTICA DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA E.S.E HOSPITAL SAN FRANCISCO DE GACHETÁ BASADA EN LA NORMA ISO 27001:2013

INTRODUCCCIÓN

Esta auditoría se realizó a los servicios de tecnologías de la información de la E.S.E Hospital San Francisco de Gachetá, bajo la norma ISO 27001:2013 y nace como parte de una problemática enfocada en la pérdida de la confidencialidad de la información y en la no realización de procesos auditoría a dichos servicios.

La realización de esta auditoría radica en el interés de la Gerencia de la Información del Hospital en conocer las vulnerabilidades de sus servicios y en el autor para contribuir a la condifencialidad de la información administrativa y asistencial, que corresponde al Hospital y a los usuarios.

Por medio de instrumentos de recolección de información, tales como entrevistas y encuestas, revisión de la documentación, procesos y procedimientos del área de seguridad de la información de la entidad y escaneo de sus redes por medio de herramientas de software se realizó un diagnóstico del estado de seguridad de la información en la Institución.

Se propone como finalidad minimizar el impacto de la pérdida de confidencialidad de información financiera y registros de historia clínica a través de la aplicación de una auditoria a la seguridad informática de los servicios de tecnologías de la información bajo la norma ISO 27001:2013 y la metodlogía Magerit V3.

Se aplicó la metodología Magerit, con el fin de realizar el respectivo análisis y gestión de amenzas, vulnerabilidades, controles, clasificación de activos, valoración cuantitativa, valoración cualitativa y tratamiento del riesgo.

El informe de auditoría contempla diversos aspectos, tales como copias de seguridad, infraestrutura de redes, acceso físico, redes inalámbricas, firewall, antivirus, contraseñas, ingeniería social, gestion de la seguridad de la información, organización y aspecto.

1. PROBLEMA

1.1 DEFINICIÓN DEL PROBLEMA

En la E.S.E Hospital San Francisco de Gacheta, se maneja una red de datos y servicios de tecnologías de la información, para los diversos servicios administrativos y asistenciales.

El problema que se pretende solucionar en la E.S.E Hospital San Francisco de Gacheta es la pérdida de la confidencialidad de la información, ya que no cuenta con la implementación de procesos de auditoría a la seguridad informática y por ende no existen informes, planes de mejoramiento ni seguimiento a los mismos. Por lo cual existen riesgos de perdida de la confidencialidad en los registros de historias clínicas y los balances financieros de la entidad.

1.2 DESCRIPCIÓN DEL PROBLEMA

La E.S.E Hospital San Francisco de Gachetá, realiza sus actividades administrativas y asistenciales, mediante un software de Información CNT, el cual está dividido por módulos: cartera, facturación, contabilidad, presupuesto, contratación, talento humano, Cirugía, paciente, laboratorio clínico, farmacia y entre otros.

La E.S.E cuenta con una estructura por procesos y unidades funcionales, la unidad funcional competente con las tecnologías de la información y las comunicaciones, se denomina gerencia de la Información, donde se cuenta con ciertos procesos, procedimientos, protocolos y políticas de seguridad de la información.

Por ello se debe garantizar por medio de procesos de auditoría, que la ejecución de los procesos de seguridad de la información, tanto de los módulos administrativos y asistenciales, se lleve a cabo de acuerdo a la normatividad y políticas aplicadas.

Desde la mirada técnica se evidencian problemas de contagio de software malicioso dentro de la red del hospital, no cumplimiento con los planes de mantenimiento de software y hardware, manejo de contraseñas no apropiadas, la no restricción de permisos en equipos del hospital y en acceso a redes, por lo cual se pierde la confidencialidad de la información, tanto en la parte financiera como en la parte asistencial de registros de historia clínica.

La preocupación a nivel de confidencialidad de la información, radica en la no ejecución de procesos de auditoría a nivel informático, puesto que las unidades funcionales de Control Interno y Gestión de Calidad se enfocan a la medición de indicadores, plan de auditorías y seguimiento a planes de mejoramiento a los procesos asistenciales, pero nunca a la Seguridad de la información.

Lo anterior conlleva a un riesgo alto de pérdida de confidencialidad de la historia clínica de los pacientes, contemplada en la Resolución 1995 de 1999 y la información financiera que pueda generar pérdidas económicas a la E.S.E, debido a falta de controles en cuanto a contraseñas y acceso a equipos, falta de mantenimiento de software y hardware.

1.3 FORMULACIÓN DEL PROBLEMA

¿Cómo el proceso de auditoría a los servicios de tecnologías de la información permitirá minimizar los riesgos relacionados con la pérdida de la confidencialidad en información financiera y registros de historia clínica en la ESE Hospital San Francisco de Gachetá?

2. JUSTIFICACIÓN

Para la Empresa Social del Estado Hospital San Francisco de Gachetá, la ejecución de este proyecto es muy importante ya que evitará inconvenientes legales y económicos en cuanto a confidencialidad de historias clínicas y balances financieros, además será un pilar en la satisfacción del cliente y la mejora continua de la calidad de los procesos.

Debido a la cantidad de información que se maneja, tanto historias clínicas e información financiera es necesario verificar mediante la aplicación de una auditoría de Seguridad informática, si las políticas establecidas y los controles actuales son efectivos y garantizan la confidencialidad.

Una entidad con tan alta responsabilidad social, necesita que la información manejada sea confidencial y por lo tanto no presente ningún tipo de modificación no autorizada que ponga en peligro el ciclo de atención de un paciente o que ponga en grave riesgo la situación financiera de la entidad. También debe garantizar que la información de cada uno de sus usuarios debe ser confidencial como lo estipula la resolución 1995 del 8 de julio de 1999.

De acuerdo con la estructura por procesos de la entidad, los usuarios internos son cada uno de los funcionarios de la planta administrativa y asistencial que ejercen funciones financieras, administrativas, de apoyo y misionales. Y los usuarios externos, los cuales corresponden a cada uno de los pacientes que requieren la prestación del servicio de salud y los proveedores.

Los usuarios internos de la Institución prestadora de servicios de salud son altamente beneficiados con la implementación de una auditoría a la seguridad informática, ya que tendrán la plena seguridad de contar con un sistema seguro, privado, accesible y confidencial. Así mismo el usuario externo será un potencial beneficiario de la aplicación de dicha auditoría, ya que permitirá establecer los

puntos neurálgicos de la confidencialidad e integridad de los datos consignados en sus historias clínicas y le asegurará el derecho a la privacidad.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Minimizar el impacto de la pérdida de confidencialidad de información financiera y registros de historia clínica a través de la aplicación de una auditoria a la seguridad informática de los servicios de tecnologías de la información en la E.S.E Hospital San Francisco de Gacheta.

3.2 OBJETIVOS ESPECÍFICOS

- Proponer un plan para la ejecución de la auditoria de seguridad informática, definiendo los métodos, técnicas, procedimientos, plan de pruebas y solicitud de documentos para que esta se lleve a cabo de forma satisfactoria.
- Identificar las amenazas y los riesgos a través de los instrumentos de recolección de información y pruebas propuestas, con el fin de medir la probabilidad de ocurrencia y el impacto dentro de la organización.
- Elaborar un dictamen de la auditoría de acuerdo a los hallazgos encontrados para medir los niveles de madurez de la organización.
- Elaborar un informe final de la auditoria con las recomendaciones para que el Hospital establezca el plan de mejoramiento y el sistema de control adecuado.

4. ALCANCE Y DELIMITACIÓN DEL PROYECTO

La aplicación de una auditoría de seguridad informática, con el fin de establecer un plan de mejoramiento para cada uno de los riesgos u oportunidades de mejora encontrados se llevará a cabo en la Empresa Social del Estado Hospital San Francisco de Gachetá Cundinamarca, II nivel de atención en salud.

Dicho proyecto se ejecutará en las unidades funcionales de Gestión documental, gerencia de la Información y en las unidades funcionales administrativas y financieras, tales como contabilidad, presupuesto, cartera, tesorería, talento humano y contratación.

Los activos a tener en cuenta en el proceso de auditoría y de acuerdo a la metodología Magerit V3, son equipos de cómputo, servidores, sistemas operativos, software de Gestión hospitalaria, recurso humano asistencial, recurso humano de apoyo, recurso humano administrativo, historias clínicas de paciente, y cada uno de los archivos financieros de la institución.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Con relación a los antecedentes se encuentran los siguientes:

Proyecto denominado “Auditoría al sistema de Gestión Informática enfocado en el hardware, software y redes del Hospital Universitario Departamental de Nariño”, presentado por Carlos Paredes en la Universidad Antonio Nariño. El proyecto presenta una revisión sistematizada del área de informática a través de la observación y entrevistas en cuanto a la estructura orgánica del Hospital. Este proyecto servirá para establecer las técnicas y procedimientos para la recolección de la información.

Proyecto denominado “Prototipo para la auditoria al sistema de gestión seguridad de la información (SGSI)”, presentado por Luisa Fernanda Momphotes y José Alexander Alzate en la Universidad Tecnológica de Pereira. El proyecto pretende desarrollar una herramienta tecnológica que facilite el desarrollo de una auditoria informática, bajo los criterios de la norma ISO/IEC 27001. Este proyecto servirá para tener claras las etapas de planeación, ejecución y dictamen final de una auditoría.

Proyecto denominado “Diseño de procedimientos de auditoría de cumplimiento de la norma NTP-ISO/IEC 17799:2007 como parte del proceso de implantación de la norma técnica NTP-ISO/IEC 27001:2008 en instituciones del estado peruano”, presentado por Fernando Miguel Huamán en la Pontificia Universidad Católica del Perú. El proyecto pretende establecer un procedimiento de auditoría de cumplimiento para la Norma Técnica Peruana NTP-ISO/IEC 17799:2007 en las instituciones del Estado Peruano basado en el marco COBIT 5.0, como parte del proceso de implantación de la Norma Técnica Peruana NTP-ISO/IEC 27001:2008 con la finalidad de mejorar la gestión de la seguridad de la información. Este

proyecto será la base para establecer los procedimientos de auditoría que deban ejecutarse.

Proyecto denominado “Auditoría de seguridad informática ISO 27001 para la empresa de alimentos ITALIMENTOS CIA. LTDA”, presentado por Miguel Cadme y Diego Fabián Duque en la Universidad politécnica Salesiana. El proyecto pretende realizar un análisis exhaustivo de los riesgos y vulnerabilidades de la compañía, con el fin de realizar un manual de políticas de seguridad, basados en la norma ISO 27001. Este proyecto servirá como base para estructurar la auditoría enfocada a la prevención del riesgo.

5.2 MARCO CONTEXTUAL

Razón social: Hospital San Francisco de Gachetá

Tipo de negocio: Empresa dedicada a la prestación de servicios de salud

Sector comercial: Prestación de servicios de salud

Reseña Histórica de la Entidad.

En la región del Guavio se empezó a contar con la atención en salud en los primeros años del siglo XX, gracias a las donaciones que un grupo de vecinos hicieron para la construcción del Hospital, el cual quedó constituido en 1905 con el carácter de particular, con el fin de prestar asistencia social a las personas que no contaban con los recursos económicos suficientes.

Por ordenanza 43 del 15 de mayo de 1933, se ordena la construcción del Hospital de Gachetá cuyo nombre fue Hospital Distrital San Antonio. Posteriormente el 20 de julio de 1954 este nombre fue cambiado por el de San Francisco en reconocimiento al Doctor Francisco Ortega, Síndico Gerente de la Junta de Beneficencia de Cundinamarca, por sus aportes en auxilios a esta institución. En 1954, se traslada

la sede del hospital del centro de la población a la nueva construcción que es la sede actual. En 1977 recibió el nombre de Hospital Regional San Francisco de Gachetá y en 1984, atendiendo a las nuevas leyes en salud, recibe el nombre de hospital San Francisco de Gachetá, II nivel.

Hasta 1985 el Hospital tuvo un crecimiento muy lento mostraba un atraso general en su tecnología.

A partir de 1986 se inició la modernización de la infraestructura y tecnología del hospital y se ofrecieron servicios con especialistas en oftalmología y cirugía plástica.

El 22 de marzo de 1996, según ordenanza número 027, se declaró el hospital como Empresa Social del Estado y su nombre es: E.S.E. Hospital San Francisco de Gachetá, II nivel. En el año 2003 se inician las modificaciones en la infraestructura y dotación de equipos en el Hospital y Centros de Salud, dando cumplimiento al decreto 2309 de 2002, de igual forma se inicia el proyecto de habilitación de servicios. En cuanto a su infraestructura tiene unas modificaciones en lo referente a cambios de cubierta, pisos en las unidades funcionales de hospitalización y urgencias, adecuación de baños para los usuarios de consulta externa, hospitalización y urgencias, adecuación del servicio de urgencias, sala de partos y trabajo de partos, central de esterilización, morgue, zona de parqueo, instalación de aire acondicionado para salas de cirugía, cambio de ventanales, remodelación y reubicación de los consultorios de odontología, laboratorio clínico y farmacia, la adquisición de nuevos equipos de tecnología avanzada para la prestación de servicios con calidad, acorde a las exigencias del Ministerio de la Protección Social, obras que se finalizan en su totalidad en el año 2005.

Luego gracias a los recursos de cuentas maestras, se procede al rediseño del área de urgencias, construcción de una unidad de cuidados intermedios, remodelación y adecuaciones locativas de la unidad funcional de Cirugía, con el fin de cumplir con las exigencias de la resolución de habilitación, traslado y adecuación de consultorios

odontológicos, oficina de atención al usuario, farmacia y la construcción de un auditorio multipropósito, obras que finalizarán en el cuarto trimestre del año 2016.

Actualmente cuenta con 38 camas distribuidas en adultos, pediatría y obstetricia. El servicio de urgencias es veinticuatro horas, cuenta con servicios de consulta externa, telemedicina, radiología de baja y mediana complejidad, pediatría, obstetricia, medicina interna, otorrinolaringología, ortopedia, odontología mediana complejidad, cirugía mediana complejidad, salas de parto, mamografía, laboratorio clínico mediana complejidad, unidad de cuidados intermedios, psicología, nutrición, fonoaudiología, fisioterapia, gimnasio, ecografías, endoscopias, colonoscopias, optometría, cafetería, rampas de acceso a discapacitados, televisión, cómodas salas de espera, circuito cerrado de televisión, amplias zonas de parqueo, zona deportiva y zonas verdes.

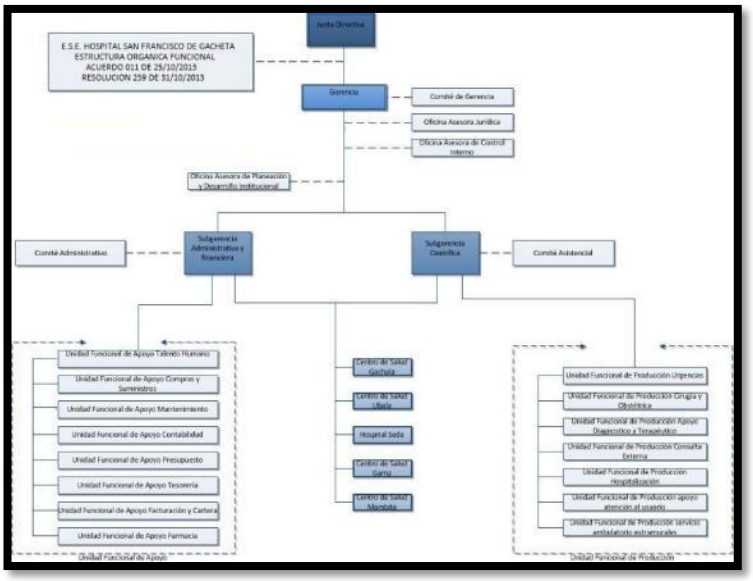
Localización.

La E.S.E. Hospital San Francisco de Gachetá esta ubicada en la carrera octava con calle sexta en el municipio de Gachetá Cundinamarca a 100 kilómetros o dos horas, de la cuidad de Bogotá.

El municipio esta situado a mil setecientos (1700) metros sobre el nivel del mar y su temperatura oscila entre los diez y nueve y veinticinco grados centígrados, su clima es templado.

El organigrama general de la empresa se encuentra a continuación.

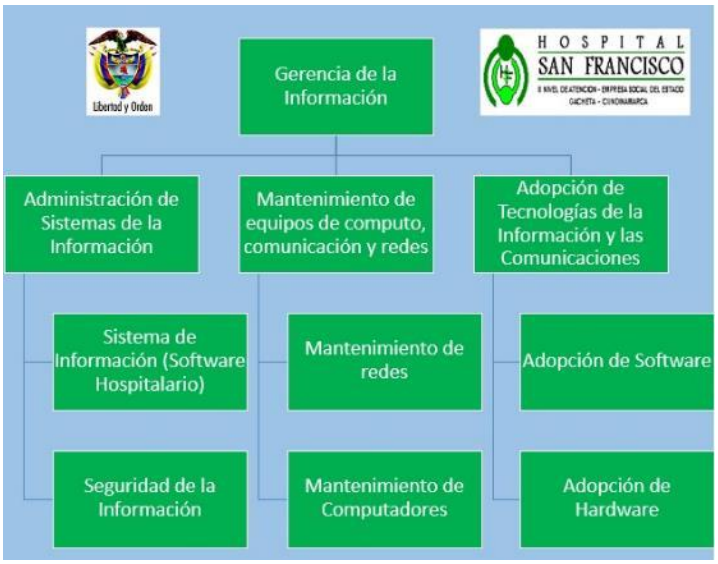
Figura 1. Organigrama general



Fuente: Carta organizacional. Hospital San Francisco de Gachetá

Descripción del área de informática o Gerencia de la Información.

Figura 2. Organigrama gerencia de la información



Fuente: Manual de Procesos y procedimientos. Hospital San Francisco de Gachetá

Dentro de la unidad funcional de gerencia de la Información, de la Empresa Social del Estado Hospital San Francisco de Gachetá, más específicamente en el área de sistemas se identifican los siguientes activos informáticos.

Tabla 1. Tabla de activos informáticos

TIPO DE ACTIVO	DESCRIPCIÓN DE LOS ACTIVOS
ACTIVO DE INFORMACION	Normatividad Institucional
	Convenios Institucionales
	Base de datos de Contratación
	Base de datos de Talento humano
	Base de datos de Historias Clínicas
	Base de datos contable
	Base de datos de Activos fijos
	Base de datos de Presupuesto
	Base de datos de cartera y facturación
	Base de datos del servicio farmacéutico
	Base de datos de Control Interno y Calidad
	Base de datos de tesorería
	Base de datos de Mantenimiento
	Base de datos de compras y suministros
SOFTWARE O APLICACIÓN	Sistema Operativo Windows 8

Tabla 1. (Continuación)

	Sistema Operativo Windows 7
	Sistema Operativo Windows XP
	Sistema operativo Windows Server 2012
	Software de Gestión Hospitalario CNT Sistemas
	Software de arquitectura AutoCAD 2009
	Paquete Office 2013
	Aplicativo de informes Piscis
	Aplicativo Telemedicina ITMS
HARDWARE	55 Computadores de escritorio HP
	8 Computadores portátiles HP
	1 Servidor local
	1 Servidor de Backup
	1 Servidor de red
RED	1 Router
	4 Switch Cysco
	1 Acces Point Linksys
EQUIPAMIENTO AUXILIAR	1 Planta Industrial 100KW
	1 UPS 20 KVA
	2 UPS 650 VA

Tabla 1. (Continuación)

INSTALACION	Cableado estructurado
	Red monofásica
	Red trifásica
SERVICIOS	Servicio de Internet Banda ancha 2MB
	Servicio continuo de soporte técnico al servicio de internet
	Servicio de soporte a Software Hospitalario CNT Systems
PERSONAL	2 Ingenieros de sistemas y redes
	1 Técnico electromecánico
	150 trabajadores en diversas dependencias

Fuente: El Autor

5.3 MARCO TEÓRICO

SEGURIDAD INFORMÁTICA

De acuerdo con Seguridad informática smr[1], la seguridad informática, es aquella que permite asegurar que los recursos de información de una organización estén accesibles con oportunidad a los usuarios, mantengan el acceso solo para el personal autorizado y esté debidamente restringido para los demás. Por otra parte, los recursos de información deben estar protegidos para evitar cualquier

[1] Seguridad informática smr. Seguridad Informática [en línea]. < https://seguridadinformaticasmr.wikispaces.com/TEMA+1-+SEGURIDAD+IFORM%C3%81TICA> [citado en 17 marzo de 2016]

modificación o daño intencionado con el fin de afectar la organización o la continuidad del negocio.

Como lo expresa COSTAS SANTOS[2], la seguridad informática tiene unos objetivos muy claros:

- Detección de amenazas y gestión del riesgo
- Garantizar el buen uso de los recursos y las aplicaciones
- Recuperar el sistema adecuadamente en caso de incidentes de seguridad, limitando pérdidas
- Cumplir el marco normativo legal

Ya que las Tecnologías de la información y las comunicaciones se han extendido en todos los ámbitos, de la sociedad como: educación, salud, finanzas, comercio, militar, agraria, etc. La informática se hace necesaria para la debida gestión y mejora de sus procesos tanto misionales como administrativos.

Pero a la par del gran desarrollo de la sociedad con las tecnologías de la información y las comunicaciones, se hace necesario en mayor medida implementar y hablar de la seguridad de la información, debido a que las organizaciones deben proteger la información, como su activo más valioso.

Como lo indica Ecured[3], dentro del mundo de la seguridad informática se encuentran una serie de terminología muy importante por conocer, ya que esta área del conocimiento tiene su propio lenguaje y su propia jerga.

- **Activo** es aquel recurso del sistema de información que permite a la organización funcionar y cumplir sus objetivos a cabalidad. Los activos pueden ser aplicaciones, equipos, recurso humano, información, servicios, etc.

[2] COSTAS SANTOS, Jesús. Seguridad y alta disponibilidad. 1 ed. Ediciones RA-MA, 2014. p. 10.
[3] Ecured. Seguridad informática [en línea]. <http://www.ecured.cu/Seguridad_Inform%C3%A1tica> [citado en 20 marzo 2016]

- **Amenazas** son eventos que pueden desencadenar un incidente en una organización de manera pues que se vea afectada en sus activos, tanto material o inmaterialmente.

De acuerdo al catálogo de amenazas de la metodología MAGERIT, las amenazas pueden ser de cuatro tipos:

Desastres naturales: tormentas eléctricas, terremotos, etc.
De origen Industrial: fuego, contaminación, etc.
Errores o fallos no intencionados: errores de usuarios, errores de administrador, etc.
Ataques deliberados: ingeniería social, suplantación de identidad, difusión de software dañino, etc.

- **Ataques** son aquellos eventos que pueden ser exitosos o pueden fracasar y su objetivo es atentar sobre el buen funcionamiento de un sistema.
- **Control** se refiere a un dispositivo o algún procedimiento que se efectúa con el fin de reducir una vulnerabilidad. Por ejemplo, la capacitación al personal de una empresa para evitar los ataques de ingeniería social.
- **Impacto** es la consecuencia que se mide al materializarse una amenaza.
- **Riesgo** hace referencia a la probabilidad de que se lleve a cabo una amenaza contra la seguridad de la información.
- **Vulnerabilidad** son aquellos aspectos que influyen sobre un activo informático, ampliando la posibilidad de que una amenaza se materialice.
- **Vulnerabilidades** de un sistema informático, pueden ser:
  - Falta de capacitación del personal en cuanto al tema
  - Falta de procedimientos y políticas
  - Contraseñas débiles
- **Desastre** es aquella incapacidad de acceso y procesamiento de la información en un negocio determinado. Por ejemplo, la pérdida de una base de datos por causa de un ataque informático es un desastre.

SISTEMA DE GESTIÓN DE SEGURIDAD INFORMÁTICA

De acuerdo con Ceeisec[4], un sistema de Gestión de la seguridad de la información es en esencia la respuesta a los objetivos de garantizar la accesibilidad, integridad y confidencialidad de la información y comprende entre otros, unos componentes esenciales como lo son:

- Política
- Estructura organizacional
- Procesos, procedimientos y protocolos
- Recursos humanos y financieros

Con esta herramienta, la gerencia o dirección de la organización puede:

- Ejecutar la política
- Cumplir los objetivos del Sistema de Gestión (integridad, confidencialidad, accesibilidad)
- Asignar responsabilidades
- Salvaguardar la información

Para la implementación de un Sistema de Gestión de Seguridad de la Información se debe:

- Compromiso de la dirección con el Sistema de gestión
- Definir alcance, límites y política
- Análisis de requisitos de seguridad de la información
- Valoración, planificación y tratamiento de riesgos
- Diseño del Sistema de Gestión de Seguridad de la Información
- Socialización del Sistema de Gestión de la Seguridad de la Infromación
- Evaluar el Sistema de Gestión de la Seguridad de la Información

[4] Ceeisec. Sistema de gestión de la seguridad de la información [en línea]. < www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf> [citado en 25 marzo 2016]

La estructura organizacional a tener en cuenta debe ser:

- Directivo de la empresa: Se compromete y aprueba recursos
- Comité de seguridad: define el alcance, planea, gestiona, verifica y actúa
- Coordinador de seguridad: coordina, controla, direcciona y reporta
- Personal técnico: administra y maneja la información
- Usuario interno final: hace uso de la información

La política de seguridad[5] debe contener:

- Compromiso claro de la dirección
- Debe ser comprendida y conocida por todos los funcionarios de la organización
- Aspectos orientados al acceso a la información
- Uso de activos físicos y lógicos
- Comportamientos ante un incidente de seguridad de la información
- Buenas prácticas para el manejo de la seguridad de la información

El análisis de requisitos y diseño del Sistema de Gestión de Seguridad Informática comprende los siguientes aspectos:

- Definir requisitos de seguridad
- Identificar los activos de acuerdo al alcance y límites del Sistema de Gestión
- Evaluar y conocer el estado de la seguridad en la Organización
- Plan de ejecución de controles de Tecnologías de la información y las comunicaciones y de la seguridad física
- Plan de revisiones
- Lista de insumos
- Procedimiento de revisiones (auditoría, supervisión y medición)

[5] Red y seguridad. Política de seguridad informática [en línea]. < redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html> [citado en 25 marzo 2016]

- Material de capacitación
- Plan de capacitaciones
- Registros de capacitación
- Resultados de adherencia a las capacitaciones
- Plan de ejecución del sistema de gestión de seguridad de la información

Norma ISO 27001:2013

Como lo describe Advisera[6], la ISO 27001:2013, es una norma emitida por la Organización Internacional de Normalización y trata la adecuada forma de gestionar la seguridad de la información en una organización.

La última revisión de la norma se efectúo en el año 2013 y se llamó ISO/IEC 27001:2013.

Puede ser implementada en cualquier tipo de organización, además está diseñada por los mejores especialistas del mundo y permite que una organización sea certificada en ISO/IEC 27001/2013.

La filosofía de las normas es la gestión del riesgo, basada en la evaluación y análisis del riesgo para luego implementar medidas de mitigación.

Para implementar la norma ISO/IEC 27001:2013 en una organización, es importante cumplir con una serie de pasos:

1) Compromiso de la dirección

2) Hacer uno de una metodología de gestión de proyectos

3) Definir el alcance del SGSI

[6] Advisera. Norma ISO 27001 [en línea]. < http://advisera.com/27001academy/es/que-es-iso-27001/> [citado en 25 marzo de 2016]

4) Política de seguridad de la información

5) Definir la metodología de evaluación de riesgos

6) Realizar la evaluación y el tratamiento de riesgos

7) Redactar la Declaración de aplicabilidad

8) Redactar el Plan de tratamiento de riesgos

9) Definir la forma de medir la efectividad de los controles y del SGSI

10) Implementar todos los controles y procedimientos necesarios

11) Implementar programas de capacitación y sensibilización

12) Ejecutar todas las operaciones diarias establecidas en la documentación del SGSI

13) Monitorear y medir el SGSI

14) Realizar la auditoría interna

15) Realizar la revisión por parte de la dirección

16) Implementar medidas correctivas

METODOLOGÍA DE GESTIÓN DEL RIESGO MAGERIT V3

Conforme lo explica Administración electrónica[7], MAGERIT es una metodología de análisis y gestión de riesgos en los sistemas de información y fue elaborada por el Consejo Superior de Administración Electrónica y fue actualizada en el año 2012 en su versión número 3.

[7] Administración electrónica. Metodología de Análisis y Gestión de riesgos de los sistemas de información [en línea].< http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html> [citado en 25 marzo de 2016]

En el proceso de análisis y gestión del riesgo, de acuerdo a la metodología anterior se establece:

- Inventario de activos clasificados en:

[D] Información

[SW] software

[HW] hardware

[COM] red

[AUX] equipamiento auxiliar

[L] instalación

[S] servicios

[P] personal

- Valoración de los activos: dicha valoración se realiza activo por activo, tanto cualitativamente como cuantitativamente.

- Dimensiones de seguridad: cada activo se debe valorar en cada una de las cinco dimensiones cualitativamente, dependiendo del nivel de importancia para la organización.

  Las dimensiones de valoración a tener en cuenta son:

  [D] Disponibilidad

  [I] Integridad de los datos

  [C] Confidencialidad de la información

  [A] Autenticidad

[T] Trazabilidad

- Criterios de valoración de activos: usualmente se utilizan los siguientes criterios:

Tabla 2. Valoración de activos

VALOR		CRITERIO
10	EXTREMO	Daño extremadamente grave
9	MUY ALTO	Daño muy grave
6-8	ALTO	Daño grave
3-5	MEDIO	Daño importante
1-2	BAJO	Daño menor
0	DESPRECIABLE	Daño irrelevante a efectos prácticos

Fuente: El autor

- Amenazas: la metodología Magerit V3, proporciona un catálogo de amenazas, dependiendo de su probailidad de ocurrencia, como causa de: desastres naturales, origen industrial, errores y fallos no intencionados, ataques deliberados.

Tabla 3. Catálogo de amenazas

CATÁLOGO AMENAZAS MAGERIT V3
[N] DESASTRES NATURALES
[N.1] Fuego
[N.2] Daños por agua
[N.7] Condiciones inadecuadas de temperatura o humedad
[N.X] Desastres naturales
[I] DE ORIGEN INDUSTRIAL
[I.6] Corte del suministro eléctrico
[I.8] Fallo de servicios de comunicaciones
[I.9] Interrupción de otros servicios y suministros esenciales
[I.10] Degradación de los soportes de almacenamiento de la información
[I.X]Desastres industriales
[E] ERRORES Y FALLOS NO INTENCIONADOS
[E.1] Errores de los usuarios
[E.2] Errores del administrador
[E.4] Errores de configuración
[E.8] Difusión de software dañino
[E.16] Introducción de falsa información
[E.15]Alteración de la información

Tabla 3. (Continuación)

[E.18] Destrucción de información
[E.19] Fuga de información
[E.21] Errores de mantenimiento / actualización de programas (software)
[E.23] Errores de mantenimiento / actualización de equipos (hardware)
[E.24] Caída del sistema por sobrecarga
[E.25] Pérdida de equipos
[E.28] Indisponibilidad del personal
[A] ATAQUES INTENCIONADOS
[A.6] Abuso de privilegios de acceso
[A.11] Acceso no autorizado
[A.14] Interceptación de información (escucha)
[A.24] Denegación de servicio
[A.25] Robo
[A.28] Indisponibilidad del personal
[A.29] Extorsión
[A.30] Ingeniería social

Fuente: El autor

- Valoración de amenazas: se debe realizar calculando la frecuencia con que pueda ocurrir y el impacto que pueda generar.

Puede establecerse una probabilidad de ocurrencia e impacto como la siguiente

Tabla 4. Valoración de impacto

IMPACTO		
MA	100	Muy alto
A	10	Alto
M	1	Medio
B	1/10	Bajo
MB	1/100	Muy bajo

Fuente: El autor

Tabla 5. Valoración de probabilidad de ocurrencia

PROBABILIDAD DE OCURRENCIA			
MA	100	Muy frecuentemente	A diario
A	10	Frecuentemente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: El autor

- Impacto potencial: debe determinarse qué nivel de riesgo asumirá la organización al no tener controles implementados.

- Salvaguardias: para cada activo deben determinarse aquellos procedimientos o mecanismos que ayuden en la reducción del riesgo.

Las salvaguardias[8] las hay de diferentes tipos y se catalogan así:

Tabla 6. Salvaguardias

EFECTO	TIPO
Preventivas	[PR] Preventivas [DR] Disuasorias [EL] Eliminatorias
Acotan la degradación	[IM] Minimizadoras [CR] Correctivas [RC] Recuperativas
Consolidan el efecto de las demás	[MN] De monitorización [DC] De detección [AW] De concienciación [AD] Administrativas

Fuente: El autor

- Impacto residual: después de reducir el impacto potencial, por medio de las salvaguardias, aún queda un impacto muy difícil de mitigar y es el impacto residual.

[8] Centro de transferencia tecnológica. Libro I método. [en línea] < http://administracionelectronica.gob.es/ctt/resources/Soluciones/184/Area%20descargas/Libro-I-Metodo.pdf?idIniciativa=184&idElemento=85 > [citado en 25 marzo de 2016]

- Riesgo residual: es aquel que debe asumir la organización, después de aplicar las salvaguardias.
- Resultados: corresponde al análisis detallado de la evaluación y gestión de riesgos.

AUDITORÍA INFORMÁTICA

La auditoría informática [9], pretende verificar el cumplimiento de una norma determinada. Para ello debe contarse con un procedimiento sistemático, secuencial, cronológico y ordenado.

Clasificación:

Las auditorías pueden ser internas, cuando el equipo auditor pertenece al ente auditado, o externa cuando el equipo auditor es independiente de la organización auditada.

La auditoría de sistemas computacionales especificada en el proyecto es la auditoría sobre la seguridad de sistemas computacionales, la cual revisa de forma técnica y especializada, la seguridad de los sistemas de cómputo, el personal y las áreas, con el fin de salvaguardar la seguridad de los equipos computacionales, redes, bases de datos y usuarios. También se revisan los planes de contingencia, medidas de prevención y la prevención de software malicioso.

Las técnicas de auditoría consisten en obtener información oral, escrita, por medio de observación directa, por medio de cálculos, por medio de herramientas informáticas y generalmente se utilizan las siguientes:

- Entrevistas, encuestas, cuestionarios
- Comprobación

[9] Universidad Nacional Abierta y a Distancia. Auditoría Informática [en línea]. < http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_27_fases_de_la_auditora_informatica_y_de_sistemas.html> [citado en 25 marzo de 2016]

- Observación e inspección
- Análisis, cálculos, tabulación
- Técnicas de auditoría asistidas por computador

Los procedimientos de auditoría corresponden al conjunto de técnicas aplicadas en forma lógica y secuencial para ejecutar las tareas y recopilar evidencia que respalde los hallazgos.

La metodología que se emplea para realizar las auditorías a sistemas informáticos, se puede resumir en las siguientes fases[10]:

- Estudio preliminar: donde se establece el grupo de trabajo, visita a la unidad informática, recopilación de información preliminar, solicitud de manuales, procedimientos, políticas, reglamentos y se entrevistan a los funcionarios.

- Revisión y evaluación de controles y seguridades: donde se analizan los diagramas de flujos de los procesos, pruebas de cumplimiento, revisión de aplicaciones en áreas críticas, revisión de copias de seguridad y revisión de la documentación.

- Examen detallado de áreas críticas: donde de acuerdo a las áreas críticas encontradas se centrará el trabajo, definiendo el plan de trabajo, metodología de trabajo, estudio y análisis profundo de cada problema encontrado.

- Comunicación de resultados: por medio del cual se elabora el informe en borrador y se discute con los ejecutivos de la organización para llegar así al informe definitivo, presentado esquemáticamente, por tablas o cuadros,

[10] Universidad Nacional Abierta y a Distancia. Módulo Auditoría de Sistemas [en línea]. < http://datateca.unad.edu.co/contenidos/90168/2014MODULO_90168_plantilla_unidad_2.pdf> [citado en 25 marzo de 2016]

donde especifique claramente los problemas encontrados, efectos y recomendaciones de la auditoría.

NAGAS, NORMAS GENERALES PARA LA AUDITORÍA DE LOS SISTEMAS DE INFORMACIÓN

Estas normas[11] cumplen un papel muy importante dentro del papel del auditor de sistemas de información y establecen:

- Se establecerá un título de auditoría que involucre autoridad y responsabilidad
- El auditor debe ser independiente y no tener ninguna relación con la organización a la cual audita
- El auditor debe acogerse al código de ética de la Asociación de Auditoría y Control de Sistemas de Información
- El auditor debe tener el conocimiento, la técnica y las habilidades para desempeñar sus tareas de auditor
- Debe planificar la auditoría, para cumplir con las normas y satisfacer los objetivos de la auditoría
- Durante la ejecución, el equipo auditor debe ser supervisado con el fin de garantizar el cumplimiento de los objetivos de la auditoría
- Durante la ejecución, el equipo auditor debe recolectar las evidencias suficientes para ser analizadas e interpretadas para sustentar los hallazgos y así garantizar el cumplimiento de los objetivos de la auditoría
- El informe entregado debe contener como mínimo: alcance, objetivos, periodo de cobertura, naturaleza, amplitud de la labor desarrollada, organización, destinatarios, restricciones, hallazgos, conclusiones, recomendaciones, y reservas.

[11] Tú guía contable. Normas de auditoria generalmente aceptadas [en línea]. <www.tuguiacontable.org/app/article.aspx?id=119> [citado en 25 de marzo de 2016]

- El auditor debe solicitar hallazgos, conclusiones y recomendaciones anteriores para determinar si se han implementado las acciones de mejora y se han realizado las acciones de seguimiento a los planes de mejoramiento.

EL PROGRAMA DE AUDITORÍA

Un programa de auditoría[12] permite esquematizar el trabajo a desarrollar, los procedimientos y los papeles de trabajo.

El programa de auditoría, debe estar correctamente alineado con los objetivos propuestos en la auditoría para asegurar suficiencia y pertinencia de la evidencia.

Los programas de auditoría deben ser realizados luego de la fase de planeación con base a la información del análisis de la organización, aunque puede ser modificado en la etapa de ejecución, pero debe ser aprobado por el supervisor de la auditoría.

Los requisitos más importantes son:

- Objetivos, alcanzables, comprensibles y medibles
- Debe permitir la iniciativa y el criterio del auditor
- Incluir información relevante para efectuar el trabajo
- Establecer tareas específicas
- Deben elaborarse en base a normas de auditoría internacionales y nacionales
- Conocer los ciclos, procesos, procedimientos, áreas y responsables de cada una de las dependencias a evaluar en la entidad

Propósitos:

- Asegurar el cumplimiento de los objetivos

[12] Unicauca. Elaboración de programas de auditoría [en línea]. < fccea.unicauca.edu.co/old/tgarf/tgarfse67.html> [citado en 25 de marzo de 2016]

- Disponer de un esquema lógico de trabajo que permita desarrollar el trabajo con coherencia
- Documentar la relación entre objetivos y procedimientos
- Identificar los criterios que se emplearán en la evaluación
- Al grupo auditor debe proporcionársele un plan de trabajo sistemático
- Asignar responsabilidades al equipo auditor para asegurar cumplimiento eficiente de las tareas
- Distribuir de forma adecuada el trabajo en el equipo siempre y cuando haya coordinación entre los integrantes
- Servir como guía para futuros trabajos

La estructura de auditoría debe contener como mínimo los siguientes ítems:

- Objetivo general y específicos de los procedimientos a desarrollar
- Criterios de auditoría y fuentes de los mismos
- Procedimientos
- Papeles de trabajo
- Período a evaluar
- Responsables de las pruebas
- Duración de la prueba

CICLO DEMING

El ciclo Deming[13], también llamado PDCA o PHVA, consta de cuatro procesos planear, hacer, verificar y actuar. Es una estrategia de mejoramiento continuo de la calidad de los procesos y es vital de llevarlo a cabo en todo sistema o proceso.

En cuanto a la seguridad informática, puede desglosarse así:

1. Planear:

[13] Universidad Nacional Abierta y a Distancia. Ciclo PDCA [en línea]. <http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html> [citado en 25 marzo de 2016]

- Estudio de la situación actual en seguridad informática

2. Hacer:
- Implantación de las medidas de seguridad

3. Verificar:
- Comprobar la efectividad y suficiencia de las medidas implantadas

4. Actuar:
- Mantenimiento
- Evaluación
- Planes de mejoramiento

5.4 MARCO CONCEPTUAL

Dentro de las auditorías informáticas, intervienen una serie de variables, la auditoría se enfoca a los controles que aplica la entidad para reducir el riesgo que una amenaza se materialice y de la eficacia de los controles depende que las variables permanezcan estables.

Algunas de las variables más importantes son:

- **ACCESIBILIDAD:** La accesibilidad de la información es uno de los factores más importantes, aunque no menos ni más que los demás descritos, ya que el usuario necesita acceder a los registros de datos en el momento exacto y sin contratiempos. Por ejemplo, en una empresa de producción, debe generarse x cantidad de producto para cumplir con un pedido especial, pero de repente se pierde el acceso a la base de datos de pedidos de los clientes y no se sabe cuántas unidades deben producirse, por ende, hay una pérdida del cliente y una pérdida económica, debido a que no se tuvo un oportuno

acceso a la información. De igual forma la vida de un paciente corre peligro ya que fue atacado con un poderoso químico, pero no se tiene acceso a la base de datos de historias clínicas para saber si el paciente es alérgico a la medicina que deberían suministrarle para salvarle la vida, ese lapso de tiempo hará que el paciente fallezca. [14]

- **AUTENTICIDAD:** La autenticidad, se refiere a la confirmación de tres patrones, el receptor, el emisor y el mensaje. Se debe verificar si el mensaje en efecto proviene del emisor que dice ser, si el mensaje es en efecto el que se quería transmitir y si llegó al receptor adecuado. El ejemplo más sencillo es la verificación que hacen los bancos, con el fin de confirmar si un cheque es auténtico, si el que lo reclama es la persona que debe reclamarlo, etc. [15]

- **INTEGRIDAD:** La integridad, es aquella propiedad de que la información sea modificada por quien esté autorizado y que el contenido de la información, o sea el mensaje a transmitir no se vea alterado. Por ejemplo, cuando se administra un medicamento a un paciente, la integridad de la información consiste en que el registro electrónico de la fórmula médica diga diez miligramos y no sea alterado, ya que, si se altera por error o por medio de un ataque deliberado, y se cambia por cien miligramos, el paciente probablemente fallecerá. [16]

[14] Tecnologías AVG. Accesibilidad [en línea]. < http://www.tecnologiasavg.com/index.php/component/k2/item/105-sistema-de-gestion-de-seguridad-de-la-informacion> [citado en 25 marzo de 2016]
[15] Universidad Nacional Abierta y a Distancia. Autenticidad [en línea]. < http://datateca.unad.edu.co/contenidos/233011/233011Exe/leccin_11_autenticidad.html> [citado en 25 marzo de 2016]
[16] Universidad Nacional Abierta y a Distancia. Integridad [en línea]. < http://datateca.unad.edu.co/contenidos/233011/233011Exe/leccin_13_integridad.html> [citado en 25 marzo de 2016]

- **CONFIDENCIALIDAD:** La confidencialidad, es uno de los aspectos más críticos de la información, ya que debe ser conocida sólo por personal autorizado y debe garantizarse que ese personal que conoce la información no vaya a divulgarla a nadie. [17]

- **PROBABILIDAD:** Es la frecuencia de ocurrencia de una amenaza, la cual puede generar un riesgo. La importancia radica en aplicar controles adecuados que sean capaces de minimizar la probabilidad de ocurrencia de una amenaza.

- **IMPACTO:** Cuando una amenaza se materializa, ocasiona un incidente o un desastre, este a su vez genera un impacto bajo, medio o alto, en las finanzas o en otros aspectos de la organización. Por ejemplo, el impacto de perder la base de datos de historias clínicas dejaría consecuencias desastrosas para la Organización.

5.5 MARCO LEGAL

LEY 1273 DE 2009 DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS: -ARTÍCULO 269A: 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 1000 salarios mínimos legales mensuales vigentes.

[17] Universidad Nacional Abierta y a Distancia. Confidencialidad [en línea]. < datateca.unad.edu.co/contenidos/233011/233011Exe/leccin_12_confidencialidad.html> [citado en 25 marzo de 2016]

LEY 1273 DE 2009 DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS: -ARTÍCULO 269C: 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 trasporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

LEY 1273 DE 2009 DE LA PROTECCIÓN DE LA INFORMACIÓN Y DE LOS DATOS: -ARTÍCULO 269D: 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 1000 salarios mínimos legales mensuales vigentes.

LEY 1266 DE 2008- ARTÍCULO 269J: El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1500 salarios mínimos legales mensuales vigentes.

La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa.

RESOLUCIÓN 1995 DE 1999, “Por la cual se establecen normas para el manejo de la Historia Clínica”

6. DISEÑO METODOLOGICO

6.1 METODOLOGÍA DE LA INVESTIGACIÓN

Para el desarrollo de la auditoría de seguridad informática a los servicios de tecnologías de la información de acuerdo a la norma ISO 27001:2013 en la E.S.E Hospital San Francisco de Gachetá, se propone el modelo de una Investigación exploratoria ya que se considera como uno de los primeros acercamientos científicos a un problema determinado. Este tipo de investigación se utiliza cuando el problema no ha sido abordado o no ha sido estudiado de forma suficiente y las condiciones existentes no son aún determinantes, lo cual aplica para este caso ya que la problemática en mención aún no ha sido estudiada en la organización, lo que genera unas condiciones que no han sido determinantes para la solución del problema.

Para el caso específico de la auditoría de seguridad informática a los servicios de tecnologías de la información de acuerdo a la norma ISO 27001:2013 en la E.S.E Hospital San Francisco de Gachetá, el enfoque de investigación es cuantitativo ya que se pretende hacer la medición de las vulnerabilidades, amenazas y riesgos en cuanto a la confidencialidad, integridad y disponibilidad de la información.

Lo anterior lleva a realizar una investigación exploratoria con enfoque cuantitativo ya que nunca se ha realizado una exploración de la problemática en seguridad informática de la E.S.E Hospital San Francisco de Gachetá y para ello se requiere de una medición de diferentes variables de seguridad informática.

- **UNIVERSO**

El universo del proyecto auditoría de seguridad informática a los servicios de tecnologías de la información de acuerdo a la norma ISO 27001:2013 en la E.S.E Hospital San Francisco de Gachetá es el personal de la institución que tiene acceso a los equipos de cómputo utilizados en cada uno de los procesos administrativos y asistenciales de cada una de las unidades funcionales de la entidad.

- **MUESTRA**

La muestra es de tipo intencional y está definida por los usuarios de los equipos de cómputo del área administrativa y de historias clínicas de la E.S.E. Hospital San Francisco de Gacheta, específicamente los equipos de cómputo de las unidades funcionales de: cartera, contabilidad, presupuesto, activos fijos, compras, tesorería, recursos humanos, contratación, facturación, gerencia de la información, historias clínicas y un equipo de consulta externa.

- **FUENTES E INSTRUMENTOS DE RECOLECCION DE LA INFORMACION**

Con el fin de realizar la recolección de información para el proyecto auditoría de seguridad informática a los servicios de tecnologías de la información en la E.S.E Hospital San Francisco de Gachetá se tomará en cuenta las siguientes fuentes e instrumentos.

Fuentes primarias:

- Personal administrativo (cartera, contabilidad, presupuesto, activos fijos, compras, tesorería, recursos humanos, contratación, facturación, historias clínicas)
- Personal asistencial (médicos y enfermeras)
- Administradores de sistemas de la información

Fuentes secundarias:

- Documentación de la unidad funcional de Gerencia de la Información del Hospital
- Documentación (manuales, procedimientos) de la unidad funcional de Historias clínicas

Instrumentos y técnicas:

- Encuesta sobre conocimientos básicos en seguridad informática
- Entrevista a las personas encargadas de los equipos de computo
- Lista de chequeo a la infraestructura tecnológica para identificar vulnerabilidades
- Lista de chequeo acerca de la documentación y adherencia a la misma por parte de los encargados del departamento de Gerencia de la información y de los usuarios de la infraestructura tecnológica

Se espera que al aplicar estos 4 instrumentos se pueda realizar un plan de mejoramiento que permita adecuar los controles de seguridad de la E.S.E Hospital San Francisco de Gachetá, de acuerdo al objetivo del proyecto.

6.2 METODOLOGIA DE DESARROLLO

- **PLANEACIÓN DE LA AUDITORÍA**

Dentro de esta etapa, se definirán los métodos, técnicas, procedimientos e instrumentos necesarios, también se elaborará el plan auditor, dentro del cual se establecen los objetivos de la auditoría, el alcance, el equipo auditor, agenda a llevar a cabo, áreas a visitar, documentos que se solicitarán y carta de solicitud ante la Gerencia de la E.S.E. Hospital San Francisco de Gachetá.

- **EJECUCIÓN DE LA AUDITORÍA**

De acuerdo a esta etapa, se acudirá al área seleccionada, se hará la presentación del equipo auditor, se dará a conocer el plan auditor, se aplicará cada uno de los instrumentos, herramientas, métodos, técnicas y procedimientos dentro del alcance de la auditoría y conforme a la agenda estipulada. Lo anterior con el fin de identificar cada una de las oportunidades de mejoramiento, que conllevarán a la elaboración del dictamen preliminar y a la puesta en discusión del mismo.

- **DICTAMEN FINAL**

En esta fase metodológica se requiere elaborar el informe final de auditoría, de acuerdo a las oportunidades de mejoramiento encontradas y conforme al dictamen preliminar.

Todo aquello con el objetivo de que el Hospital pueda establecer un plan de mejoramiento que integre un sistema de control adecuado para reducir las vulnerabilidades encontradas dicha institución.

7. RESULTADOS Y DISCUSIÓN

7.1 PLAN DE AUDITORÍA

Objetivos de la auditoría:

- Seleccionar los instrumentos de auditoría más eficaces, con el fin de realizar un excelente análisis de los procesos auditados.
- Determinar las áreas a visitar y documentos necesarios para llevar a cabo un correcto procedimiento de auditoría, que permita definir las oportunidades de mejora del área informática de la E.S.E. Hospital San Francisco de Gachetá
- Definir el plan de pruebas a ejecutar en la E.S.E. Hospital San Francisco de Gachetá, con el fin de examinar los aspectos más críticos de la seguridad de la Información.

Alcance: la auditoría de seguridad informática, se llevará a cabo en las unidades funcionales de Gestión documental, gerencia de la Información y en las unidades funcionales administrativas y financieras, tales como contabilidad, presupuesto, cartera, tesorería, talento humano y contratación de la E.S.E. Hospital San Francisco de Gachetá.

Equipo auditor: Ingeniero Francisco Javier Hilarión Novoa

Agenda a llevar a cabo: la agenda a llevarse a cabo para la ejecución de la auditoría se contempla en la siguiente tabla. En ella se estipula la fecha, las actividades de auditoría a ejecutar y cada una de las áreas auditadas. Dichas áreas son Gestión documental, gerencia de la Información, contabilidad, presupuesto, cartera, tesorería, talento humano y contratación.

Tabla 7. Agenda.

Fecha	Actividades de Auditoría	Áreas auditadas
4 de octubre 2016	Presentación del auditor y presentación del plan de auditoría	Gestión documental, gerencia de la Información, contabilidad, presupuesto, cartera, tesorería, talento humano y contratación
4 de octubre 2016	Aplicación de Encuestas en las unidades funcionales de la E.S.E.	Gestión documental, gerencia de la Información, contabilidad, presupuesto, cartera, tesorería, talento humano y contratación
4 de octubre 2016	Aplicación de entrevista al líder de Gerencia de la Información de la E.S.E. Hospital San Francisco de Gachetá	Gerencia de la Información
5 de octubre 2016	Aplicación del aplicativo de captura de paquetes wireshark	Gerencia de la Información

Tabla 7. (Continuación)

5 de octubre 2016	Aplicación del rastreador de puertos “nmap” y verificación de vulnerabilidades	Gerencia de la Información
5 de octubre 2016	Auditoría de Red WiFi	Gerencia de la Información
6 de octubre 2016	Aplicación de lista de chequeo ISO 27001:2013	Gestión documental, gerencia de la Información, contabilidad, presupuesto, cartera, tesorería, talento humano y contratación
30 de octubre 2016	Socialización del Informe de auditoría	Gerencia de la Información

Fuente: El autor

Áreas a visitar: Gestión documental, gerencia de la Información, contabilidad, presupuesto, cartera, tesorería, talento humano, contratación y portería.

Documentos requeridos:

- Sistema de Gestión de Seguridad Informática
- Certificación de estudios del Líder de Gerencia de la Información
- Inventario de activos informáticos
- Matriz de riesgos de Seguridad Informática
- Planes de mejoramiento de Seguridad Informática
- Plan de contingencia Seguridad de la Información

- Procedimiento de asignación de credenciales a los usuarios
- Procedimiento de asignación de contraseñas a la red WIFI
- Procedimiento de ingreso del personal a la Institución
- Procedimiento de egreso del personal a la Institución
- Procedimiento de generación de contraseñas
- Procedimiento de ejecución de Backups
- Procedimiento de Manejo de discos extraíbles
- Procedimiento de control de acceso a internet
- Cronograma de mantenimiento de activos informáticos
- Reportes de mantenimiento de activos informáticos
- Hojas de vida de activos informáticos
- Compromiso de confidencialidad firmado por funcionarios
- Actas de capacitación a los usuarios internos en Seguridad Informática
- Fotografías de capacitación a los usuarios internos en Seguridad Informática

7.2 PLAN DE PRUEBAS

Dentro de las pruebas contempladas, se encuentran las pruebas sustantivas y las pruebas de cumplimiento.

Las pruebas sustantivas corresponden a:

- Encuesta a líderes de unidades funcionales (Anexo A)
- Entrevista al líder de Gerencia de la Infromación (Anexo B)

Las pruebas de cumplimiento corresponden a:

- Aplicación de la lista de chequeo ISO 27001:2013 (Anexo C)
- Captura de paquetes: se realizará por medio de la herramienta Wireshark, la cual permite apturar los paquetes que viajan por la red.

  El plan del test contempla:

- Se conecta un computador portátil a la red del hospital
- Se inicia la máquina virtual VM Virtual Box
- Se carga el Sistema Operativo kali Linux en la máquina virtual
- Se ejecuta el aplicativo de captura de paquetes Wireshark
- Se capturan los paquetes por la interfaz ethernet

- Rastreador de puertos: se hará uso de la herramienta nmap, con el fin de determinar: computadoras y servidores en red, puertos abiertos, servicios en ejecución, sistema operativo, versión del sistema operativo y características del hardware de red.

  El Plan del test contempla:
  - Se inicia un computador portátil conectado a la red del Hospital
  - Se inicia el aplicativo Virtual Box, máquina virtual
  - Se inicializa el Sistema Operativo Kali Linux en modo Live
  - Se inicia el terminal de comandos en modo super usuario
  - Se inicia el aplicativo nmap para escanear puertos
  - Se ejecutan los comandos nmap respectivamente

- Escaneo de vulnerabilidades: se hará uso de la herramienta nmap, con el fin de determinar cada una de las vulnerabilidades del sistema en cuestión y que podrían ser utilizadas por un atacante con el fin de cometer un delito informático y causar impacto en la organización.

  El Plan del test contempla:
  - Se inicia un computador portátil conectado a la red del Hospital
  - Se inicia el aplicativo Virtual Box, máquina virtual
  - Se inicializa el Sistema Operativo Kali Linux en modo Live
  - Se inicia el terminal de comandos en modo super usuario
  - Se inicia el aplicativo nmap para escanear vulnerabilidades

- Se ejecutan los comandos nmap respectivamente

- Análisis de red Wifi: este análisis de auditoría permitrá determinar; hardware de red, evaluación de la señal fuera de la organización, Cifrado en uso y contraseñas utilizadas.

  El plan del test contempla:

  - Identificar la señal wifi
  - Identificar el SSID
  - Conectarse a la red
  - Verificar la contraseña de la red
  - Comprobar que tipo de cifrado se usa
  - Verificar la potencia de la red wifi

7.3 INSTRUMENTOS APLICADOS

Los instrumentos que se aplicaron fueron los siguientes:

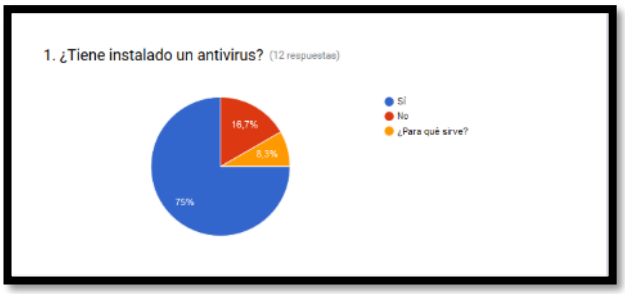
7.3.1 Encuesta

Encuesta: se realizó una encuesta a una muestra de la población de la E.S.E Hospital San Francisco de Gachetá, acerca de conocimientos básicos en Seguridad Informática. Ver Anexo A.

De la encuesta se deduce que:

El 75% de los encuestados tiene instalado un antivirus, el 16.7% no tiene instalado un antivirus y el 8.3% de los encuestados no conoce qué es un antivirus. Tal información se refleja en la siguiente figura.

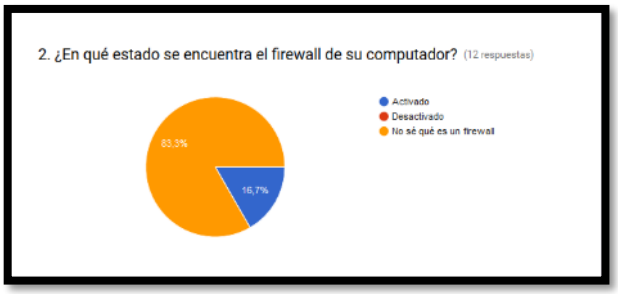
Figura 3. Pregunta 1



Fuente: El autor

El 83.3% de los encuestados no sabe que es un firewall y el 16.7% tiene activado un cortafuegos (firewall) en su computador.

Figura 4. Pregunta 2



Fuente: El autor

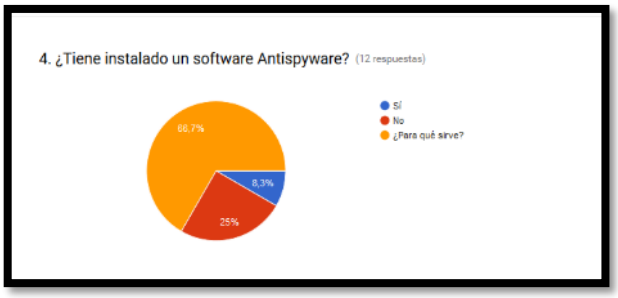
El 83.3% de los encuestados no analiza su computador con un antivirus, el 8.4% analiza su computador una vez por mes, mientras que el 8.3% analiza su computador una vez por semana.

Figura 5. Pregunta 3

Fuente: El autor

El 66.7% de los encuestados, no sabe para que sirve un software antispyware, el 25% no tiene instalado un antispyware y el 8.3% si tiene instalado un antispyware.

Figura 6. Pregunta 4



Fuente: El autor

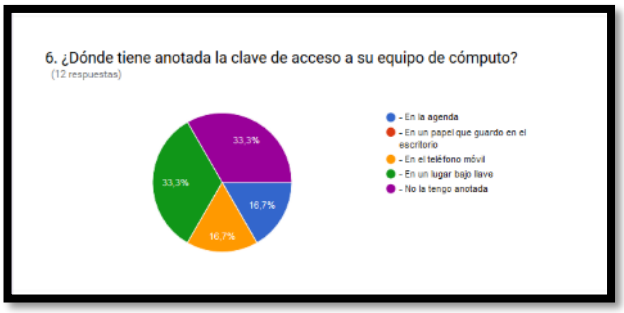
El 66.7% de los encuestados no tiene una copia de seguridad de la información, mientras que el 33.3% si tiene una copia de seguridad de su información.

Figura 7. Pregunta 5

Fuente: El autor

El 33.3% de los encuestados tiene anotada la contraseña en un lugar que esta bajo llave, el 33.3% de los encuestados no tiene anotada la contraseña en ningún lugar, el 16.7% la tiene anotada en una agenda, mientras que el 16.7% la tiene anotada en un teléfono móvil.

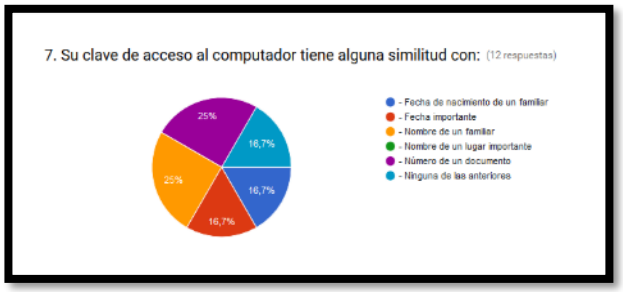
Figura 8. Pregunta 6



Fuente: El autor

El 25% de los encuestados tiene una contraseña que tiene cierta similitud con el número de documento, el 25% tiene una contraseña que tiene similitud con el nombre de un familiar, el 16.7% tiene similitud con la fecha de nacimiento de un familiar, el 16.7% tiene similitud con una fecha importante y el restante 16.7% no tiene similitud con ninguna de las anteriores.

Figura 9. Pregunta 7



Fuente: El autor

El 50% de los encuestados afirma que su contraseña de acceso tiene una combinación de números y letras, el 33.3% afirma que tiene sólo números y el 16.7% afirma que sólo tiene letras.

Figura 10. Pregunta 8

Fuente: El autor

7.3.2 Entrevista al lider de gerencia de la información

Entrevista: al líder de gerencia de la información, acerca de los procesos y procedimientos que se llevan a cabo en el área. Ver Anexo B.

De esta entrevista se concluye que no existe un Sistema de Gestión de la Seguridad de la información, prácticamente todos los procedimientos del área se realizan empíricamente sin estar debidamente documentados, no hay una matriz de gestión de riesgo informático, existe un plan de mantenimiento para el área y no hay planes de mejoramiento para esta unidad funcional

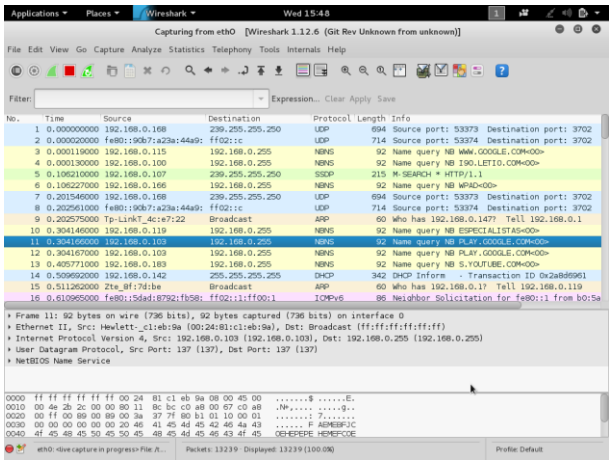
7.4 PRUEBAS DE CAPTURA DE PAQUETES

- Pruebas sobre la infraestructura utilizando kali Linux y sus herramientas de análisis y captura de paquetes.

Pruebas realizadas con el software Wireshark:

En este caso se analiza que el Host 192.168.0.103, que corresponde a un teléfono móvil, esta conectado a la red wifi y esta haciendo consultas a Google Play, lo cual es evidencia de teléfonos móviles conectados a la red realizando actualización de aplicaciones desde la tienda de Android.

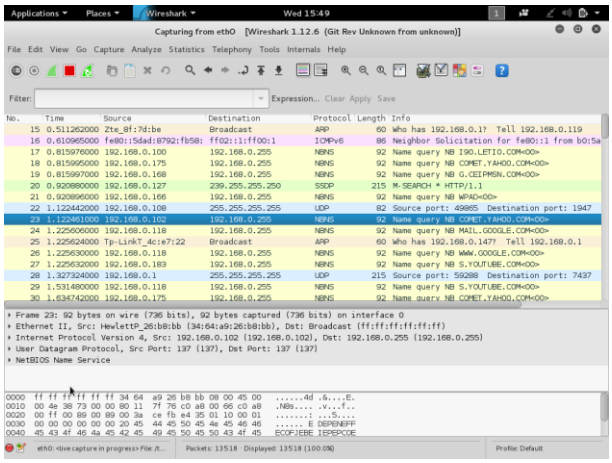
Figura 11. Consultas a Google Play



Fuente: El autor

En este caso se analiza que el Host 192.168.0.102, esta haciendo consultas a Yahoo.com. Lo cual indica que se usan los servicios de Yahoo por algunos funcionarios del Hospital.

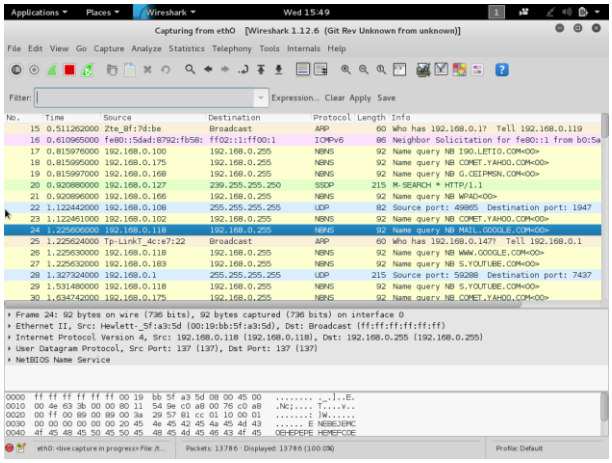
Figura 12. Consultas a Yahoo



Fuente: El autor

En el siguiente caso se evidencia que el Host 192.168.0.118, esta haciendo consultas a mail.google.com. Lo que indica que los funcionarios del Hospital usan los servicios de correo de Gmail.

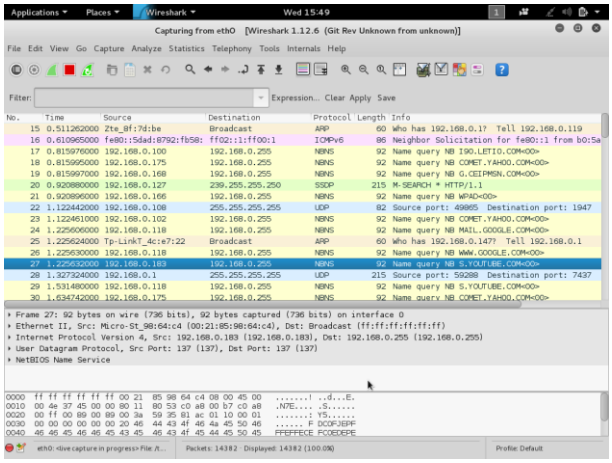
Figura 13. Consultas a mail.google.com



Fuente: El autor

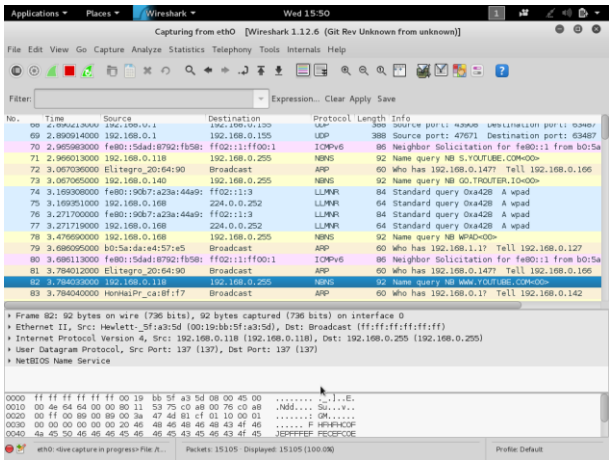
En este caso se evidencia que el Host 192.168.0.183 y 192.168.0.118, estan haciendo consultas a youtube.com. Lo cual indica que los funcionarios del Hospital acceden a YouTube para la visualización de vídeos y por ende se satura el canal de internet afectando la disponibilidad de la información.

Figura 14. Consultas a youtube.com



Fuente: El autor

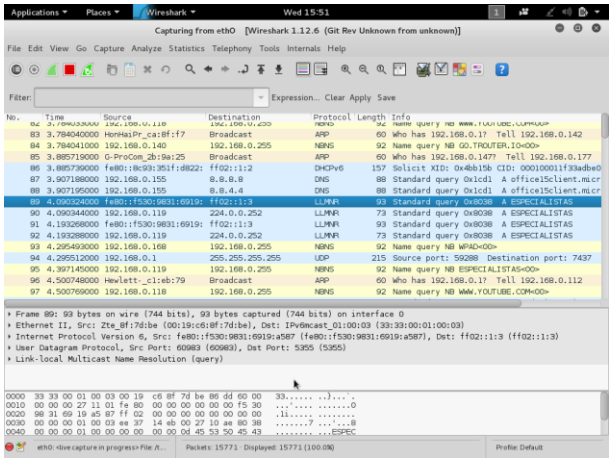
Figura 15. Otras consultas a youtube.com



Fuente: El autor

En este caso se evidencia que el Host 192.168.0.119, esta haciendo consultas a un Host llamado ESPECIALISTAS, de aquí se deduce que es muy sencillo para un intruso conocer la dirección IP del equipo Especialistas y con ello ubicar un blanco fácil y acceder a información confidencial.

Figura 16. Consultas a Especialistas

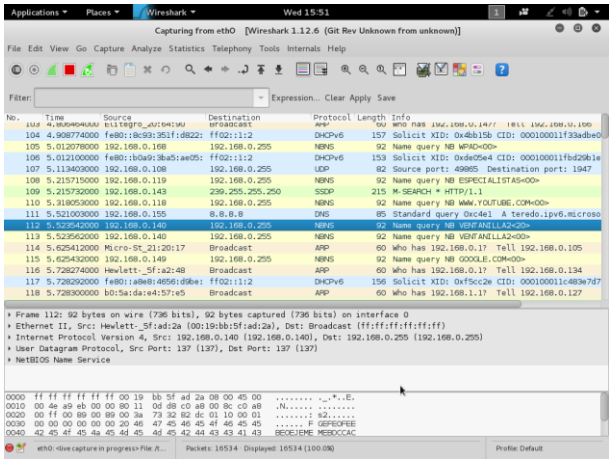


Fuente: El autor

En este caso se evidencia que el Host 192.168.0.140, esta haciendo consultas a un Host llamado VENTANILLA2, de aquí se deduce que es muy sencillo para un

intruso conocer la dirección IP del equipo Ventanilla 2 y con ello ubicar un blanco fácil y acceder a información confidencial.

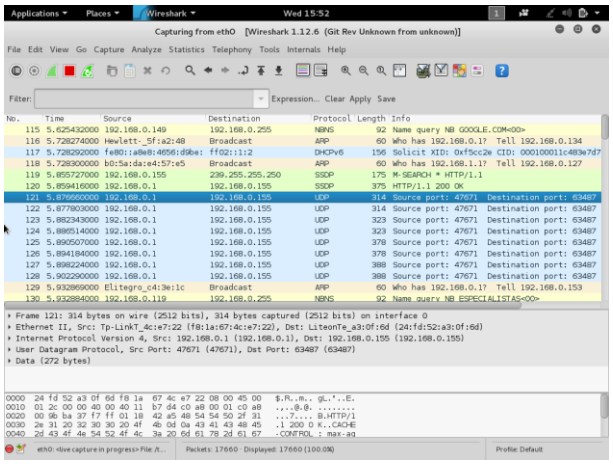
Figura 17. Consultas a ventanilla2



Fuente: El autor

En este caso se evidencia que se establece una comunicación por medio del protocolo UDP entre 192.168.0.1 y 192.168.0.155, de un puerto fuente: 47671 a un puerto destino: 63487, allí se evidencia un protocolo de control de transmisión lo cual no es motivo de preocupación.

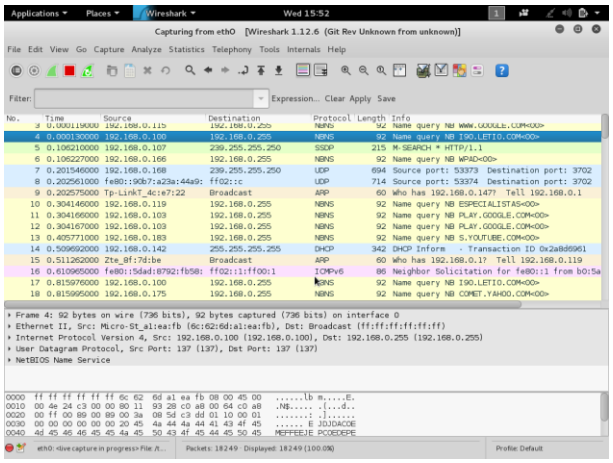
Figura 18. Comunicación UDP



Fuente: El autor

En este caso se evidencia que el Host 192.168.0.100, esta haciendo consultas a un sitio web letio.com, lo cual es prueba de que los funcionarios del Hospital están haciendo uso de servicios de radio online y ello afecta el canal de internet, favoreciendo una indisponibilidad de la información.

Figura 19. Consultas a letio.com

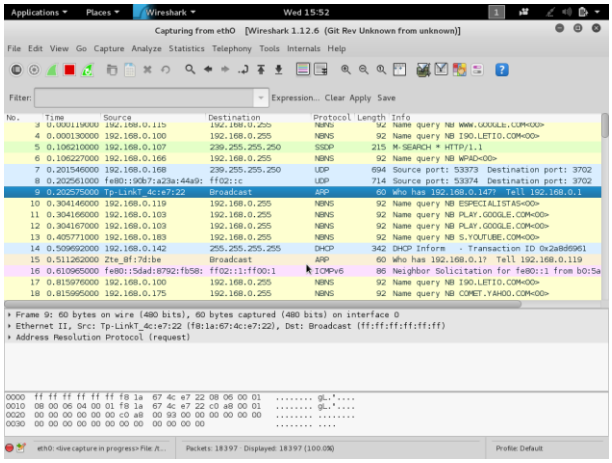


Fuente: El autor

En este caso se evidencia que el Router es de marca TP-Link y esta preguntado quien tiene la IP 192.168.0.147, lo cual puede dar pistas a un intruso de los

algoritmos de enrutamiento del Router TP-Link y como pueden aprovecharse para explotar las vulnerabilidades de este tipo de dispositivos de red.

Figura 20. Router TP-Link



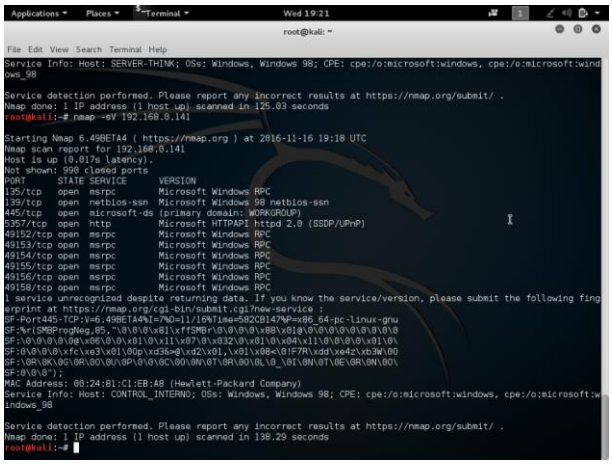
Fuente: El autor

7.5 PRUEBAS CON SCANNER DE PUERTOS

Se procede a realizar el escaneo de puertos con NMAP:

Se procede a realizar un escaneo a los puertos del HOST 192.168.0.141 que pertenece al área de Control Interno y se encuentran los puertos 135, 139, 445, 5357, 49152, 49153, 49154, 49154, 49155, 49156, 49157, 49158, que corresponden a los servicios de msrpc, netbios-ssn, Microsoft-ds, http; en estado abierto. De lo anterior se infiere que, al haber varios puertos abiertos, es muy factible aceder al equipo, ya que se pueden inyectar exploits o troyanos. El anterior procedimiento se evidencia en la siguiente figura.

Figura 21. Escaneo a computador Control Interno



Fuente: El autor

Se procede a realizar un escaneo a los puertos del HOST 192.168.0.3 que pertenece al Servidor principal del programa de Gestión de pacientes y gestión administrativa, así como las historias clínicas de paciente y se encuentran los puertos 53, 80, 88, 135, 139, 389, 445, 464, 593, 636, 1433, 2179, 2383, 3268, 3269, 3389, 49152, 49153, 49154, 49154, 49155, 49156, 49157, 49158, que corresponden a los servicios de domain, http, kerberos-sec, msrpc, netbios-ssn, ldap, Microsoft-ds, kpasswd5?, ncacn_http, tcpwrapped, ms-sql-s, vmrdp? y ms-wbt-server?; en estado abierto.

Se maneja Microsoft DNS, Microsoft HTTPAPI 2.0, Windows 2003 kerberos, Microsoft Windows RPC, dominio promario: HSFG, Microsoft SQL Server 2012 SP1 y Microsoft Windows 98 netbios-ssn. De lo anterior se infiere que, al haber varios puertos abiertos, es muy factible aceder al equipo, ya que se pueden inyectar exploits o troyanos. También es evidente que se están ejecutando los servicios de http por el puerto 80 y mysql por el puerto 1433, por ello se puede colocar un sniffer a escuchar en aquellos puertos, analizar vulnerabilidades y explotarlas. Adicionalmente pueden lanzarse ataques de inyección SQL al servidor de mysql. El procedimiento anterior se evidencia en la siguiente figura.

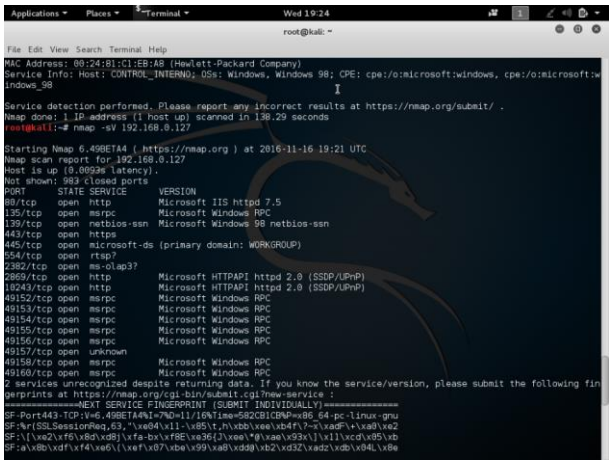
Figura 22. Escaneo a servidor principal

Fuente: El autor

Se procede a realizar un escaneo a los puertos del HOST 192.168.0.127 que pertenece al equipo de Sistemas o gerencia de la información y se encuentran los puertos 53, 80, 88, 135, 139, 389, 445, 464, 593, 636, 1433, 2179, 2383, 3268, 3269, 3389, 49152, 49153, 49154, 49154, 49155, 49156, 49157, 49158, que corresponden a los servicios de domain, http, kerberos-sec, msrpc, netbios-ssn, ldap, Microsoft-ds, kpasswd5?, ncacn_http, tcpwrapped, ms-sql-s, vmrdp? y ms-wbt-server?; en estado abierto.

Se maneja Microsoft DNS, Microsoft HTTPAPI 2.0, Windows 2003 kerberos, Microsoft Windows RPC, dominio promario: HSFG, Microsoft SQL Server 2012 SP1 y Microsoft Windows 98 netbios-ssn. De lo anterior se infiere que, al haber varios puertos abiertos, es muy factible aceder al equipo, ya que se pueden inyectar exploits o troyanos. También es evidente que se están ejecutando los servicios de http por el puerto 80 y mysql por el puerto 1433, por ello se puede colocar un sniffer a escuchar en aquellos puertos, analizar vulnerabilidades y explotarlas. Adicionalmente pueden lanzarse ataques de inyección SQL al servidor de mysql. El anterior procedimiento se evidencia en la siguiente figura.

Figura 23. Escaneo equipo Gerencia de la Información

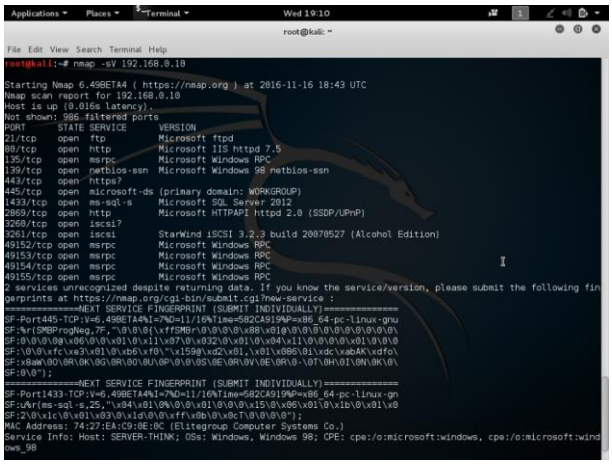


Fuente: El autor

Se realiza un escaneo de puertos al equipo servidor de reportes, identificado con la dirección IP 192.168.0.10, en el cual se encuentran los puertos 21, 80, 135, 139, 443, 445, 1433, 2869, 3260, 3261, 49152, 49153, 49154, 49154, 49155, que corresponden a los servicios de ftp, http, msrpc, netbios-ssn, Microsoft-ds, ms-sql-s; en estado abierto.

Se maneja, Microsoft ftpd, Microsoft IIS httpd 7.5, Microsoft Windows 98 netbios-ssn, Microsoft HTTPAPI 2.0, Microsoft Windows RPC, Microsoft SQL Server 2012 SP1. Dominio primario: Workgroup. De lo anterior se infiere que, al haber varios puertos abiertos, es muy factible aceder al equipo, ya que se pueden inyectar exploits o troyanos. También es evidente que se están ejecutando los servicios de http por el puerto 80 y mysql por el puerto 1433, por ello se puede colocar un sniffer a escuchar en aquellos puertos, analizar vulnerabilidades y explotarlas. Adicionalmente pueden lanzarse ataques de inyección SQL al servidor de mysql. El anterior procedimiento se evidencia en la siguiente figura.

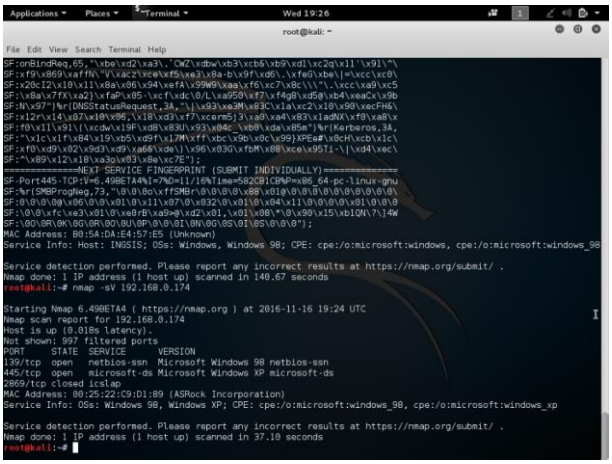
Figura 24. Escaneo de puertos equipo servidor de reportes



Fuente: El autor

Se realiza un análisis de vulnerabilidades y escaneo de puertos al equipo de estadísticas y gestión de historias clínicas de pacientes, identificado con la dirección IP 192.168.0.174, allí se encuentran los puertos 139, 445 y 2869 en estado abierto; allí se ejecutan los servicios de netbios-ssn y Microsoft-ds en sus versiones Microsoft Windows 98 netbios-ssn y Microsoft Windows XP miccrosoft-ds. En este caso el puerto 445 expone al usuario a ataques por medio de exploits, Kali Linux brinda herramientas a través de Metasploit para aprovechar las vulnerabilidades de este puerto y atacarlas.

Figura 25. Escaneo equipo estadísticas

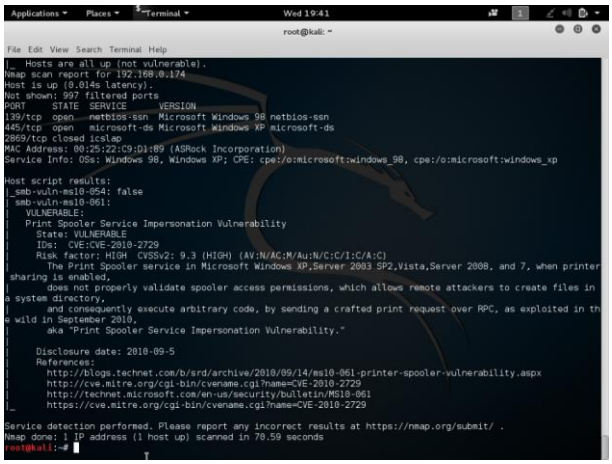


Fuente: El autor

Posteriormente se aplica un procedimiento de verificación de vulnerabilidades para el host de historias clínicas, para analizar los respectivos campos, por medio de los cuales puede colarse una explotación.

Para este caso se analizan los resultados de las vulnerabilidades encontradas. Se encuentra una vulnerabilidad en Print Spooler Service Impersonation Vulnerability y su factor de riesgo es alto. Además, la clase de vulnerabilidad pertenece a desbordamiento de búfer y es explotable a nivel remoto, lo cual indica que el equipo puede controlarse a distancia. Dicha evidencia se encuentra en la siguiente figura.

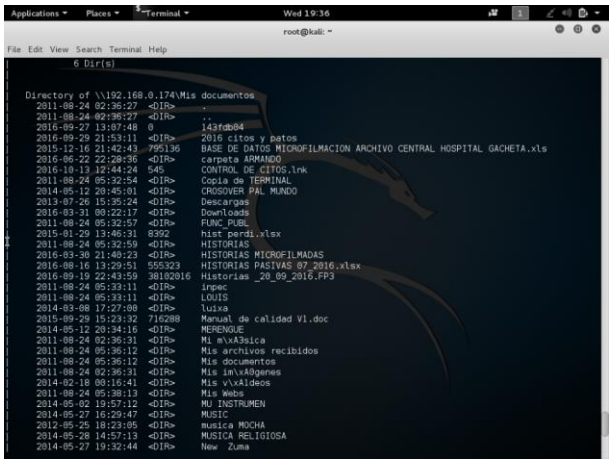
Figura 26. Resultado de vulnerabilidad del equipo de Historias Clínicas



Fuente: El autor

En este caso se acccede al directorio de archivos del equipo de historias clínicas, lo cual indica que el host es bastante vulnerable y desde allí se puede verificar los archivos de mayor potencial a atacar.

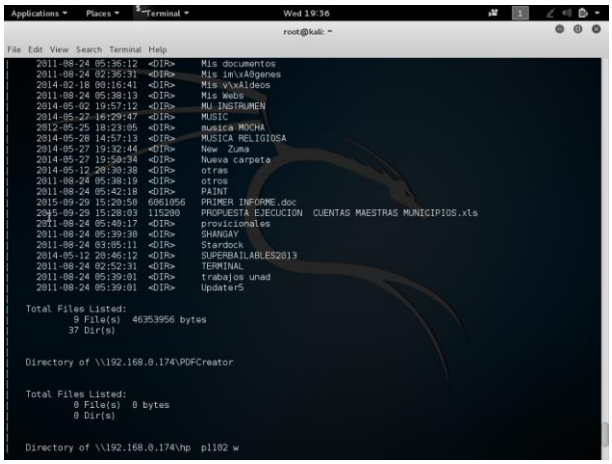
Figura 27. Archivos del equipo de Historia Clínica



Fuente: El autor

Se continúa verificando el directorio de archivos del equipo de historias clínicas.

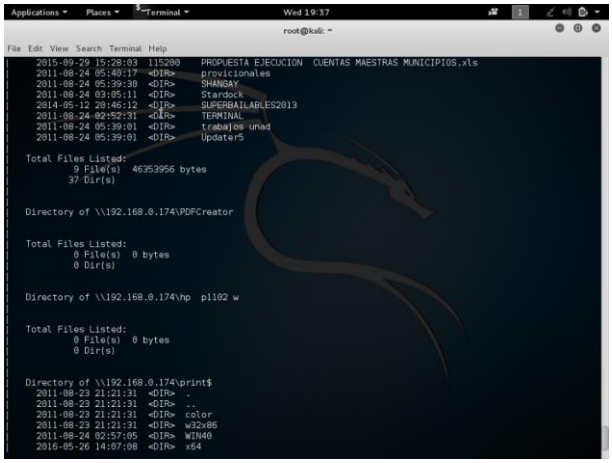
Figura 28. Archivos del equipo de Historias Clinicas II



Fuente: El autor

Por último, se lista el total de directorios que se encontraron en dicho equipo.

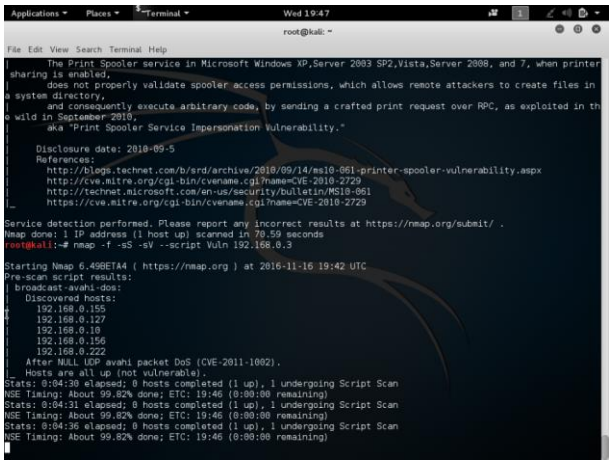
Figura 29. Directorios del equipo de Historias Clínicas



Fuente: El autor

Se ejecuta un análisis de vulnerabilidades al servidor de reportes de la institución, por medio de la herramienta nmap del sistema operativo Kali Linux.

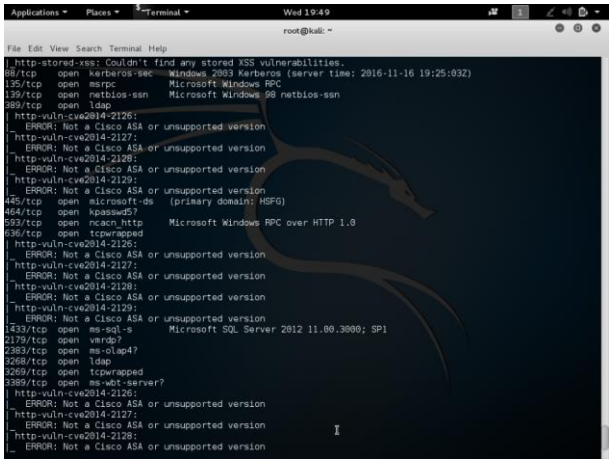
Figura 30. Escaneo de vulnerabilidades al servidor de reportes



Fuente: El autor

En este caso se revisan las vulnerabilidades encontradas por medio del lanzamiento del script de vulnerabilidades.

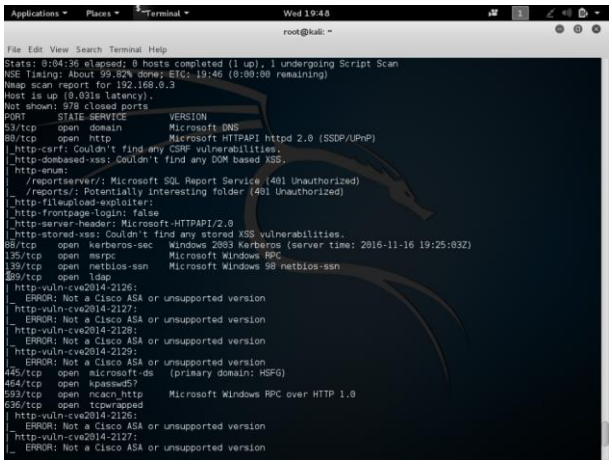
Figura 31. Vulnerabilidades del servidor de reportes



Fuente: El autor

Esta es la continuación de las vulnerabilidades encontradas.

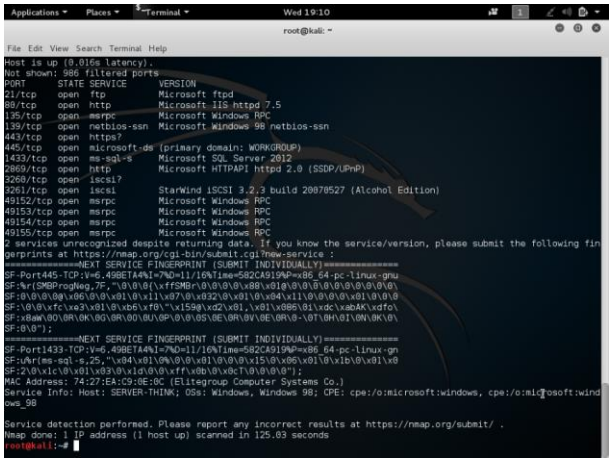
Figura 32. Vulnerabilidades del servidor de reportes II



Fuente: El autor

A continuación, se encuentran los estados de los puertos abiertos y cerrados del servidor de reportes y los servicios que corren en cada uno de ellos.

Figura 33. Puertos abiertos del servidor de reportes



Fuente: El autor

De acuerdo al análisis anterior y escaneo de puertos se puede concluir que se encuentran los puertos 21, 80, 135, 139, 443, 445, 1433, 2869, 3260, 3261, 49152,

49153, 49154, 49154, 49155, que corresponden a los servicios de ftp, http, msrpc, netbios-ssn, Microsoft-ds, ms-sql-s; en estado abierto.

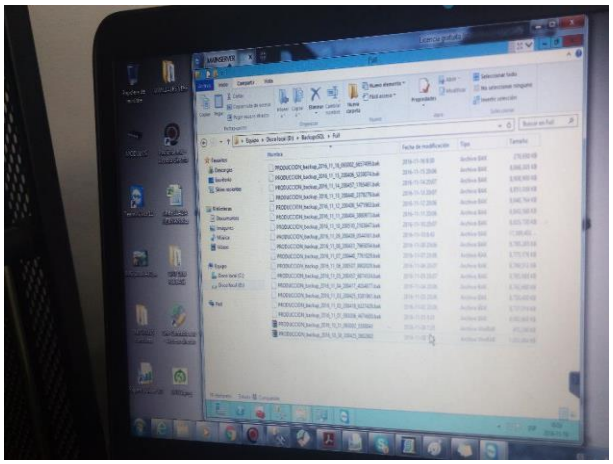
Se maneja, Microsoft ftpd, Microsoft IIS httpd 7.5, Microsoft Windows 98 netbios-ssn, Microsoft HTTPAPI 2.0, Microsoft Windows RPC, Microsoft SQL Server 2012 SP1. Dominio primario: Workgroup. El nombre del Host es Server-Think, Sistema operativo Windows. De lo anterior se infiere que, al haber varios puertos abiertos, es muy factible aceder al equipo, ya que se pueden inyectar exploits o troyanos. También es evidente que se están ejecutando los servicios de http por el puerto 80 y mysql por el puerto 1433, por ello se puede colocar un sniffer a escuchar en aquellos puertos, analizar vulnerabilidades y explotarlas. Adicionalmente pueden lanzarse ataques de inyección SQL al servidor de mysql. El anterior procedimiento se evidencia en la anterior figura.

En conclusión se evidencia que entre los puertos más comunes están el 21, donde se ejecutan los servicios ftp, el 80 para el servicio http, el 443 para el servicio mysql y en ellos se pueden usar diversos sniffer, analizadores de vulnerabilidades como nessus y nmap y posteriormente aplicar herramientas de Kali Linux, con el fin de explotar las vulnerabilidades, entre estas herramientas están Armitage y Metasploit, las cuales permiten tomar el control de la víctima violando la disponibilidad, confidencialidad e integridad de la información.

7.6 REVISIÓN DE ASPECTOS FÍSICOS

Evidencia de las copias de seguridad que se adelanta diariamente en la Institución. El procedimiento requiere de 3 copias de seguridad al día, información que se almacena en el disco duro del servidor. Luego en la tarde se graba en un DVD, con la última copia de seguridad del día y se almacena en la misma oficina.

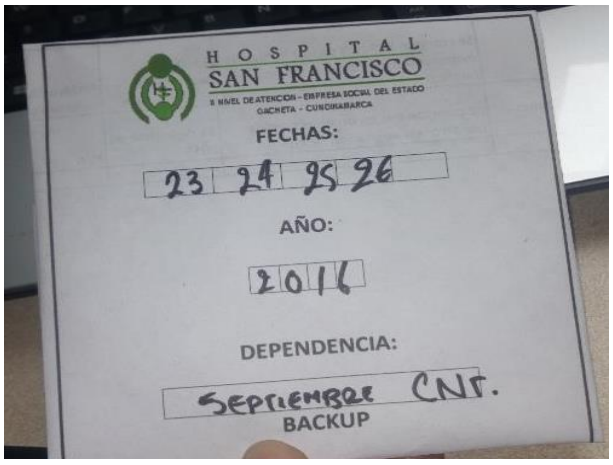
Figura 34. Copias de seguridad almacenadas



Fuente: El autor

En la siguiente figura se evidencia el etiquetado de las copias de seguridad de cada uno de los días. Sin embargo, no fue posible realizar una prueba de recuperación de desastres usando un backup, ya que no fue permitido por el Lider de Gerencia de la información.

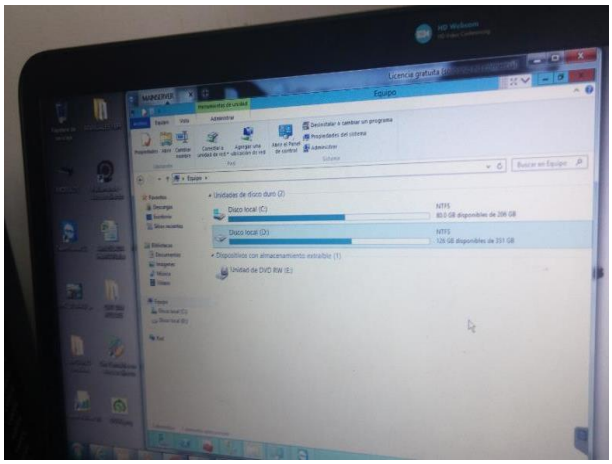
Figura 35. Etiquetado de copias de seguridad



Fuente: El autor

Evidencia de la capacidad de almacenamiento del servidor de 500 GB.

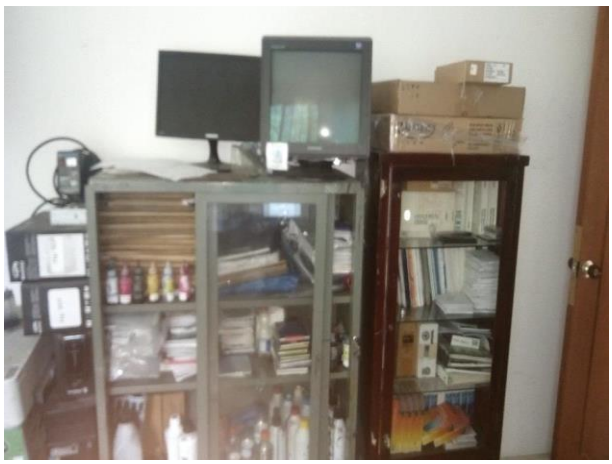
Figura 36. Capacidad del servidor principal



Fuente: El autor

Se evidencia una instantería, donde se almacenan repuestos de mantenimiento, documentación, cajas, discos, papelería y las copias de seguridad. Siendo este un logar no adecuado para su almacenamiento, ya que no cuenta con niveles de seguridad ni conservacion. No se deben mezclar, se evidencia desorden y desorganización.

Figura 37. Estantería del almacenamiento de copias de seguridad



Fuente: El autor

Se evidencia mezcla de tinta, repuestos y documentación.

Se evidencian repuestos y activos de hardware en el piso, lo cual afecta el uso, crea desorganización y mal aspecto.

Figura 38. Equipos almacenados en el piso

Fuente: El autor

Se evidencian cajas con equipos, repuestos y demás elementos que no deben estar en la oficina de gerencia de la información.

Figura 39. Almacenamiento de cajas

Fuente: El autor

Se evidencia buena ventilación, seguridad en la oficina, buenas condiciones de luminosidad ambiental y cámara de seguridad.

Figura 40. Seguridad del área de Gerencia de la Información

Fuente: El autor

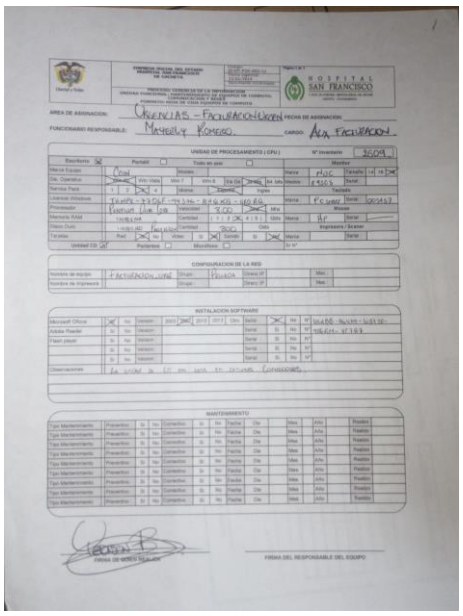
Evidencia de reporte de mantenimiento sin los principales ítems que debe llevar un reporte, para describir el equipo al cual se le realizo, numero de inventario, serial y descripción específica de la tarea realizada.

Figura 41. Reporte de mantenimiento

Fuente: El autor

En la siguiente figura se evidencia un formato de hoja de vida de equipo de cómputo, el cual tiene los ítems necesarios para su gestión e información.

Figura 42. Hoja de vida



Fuente: El autor

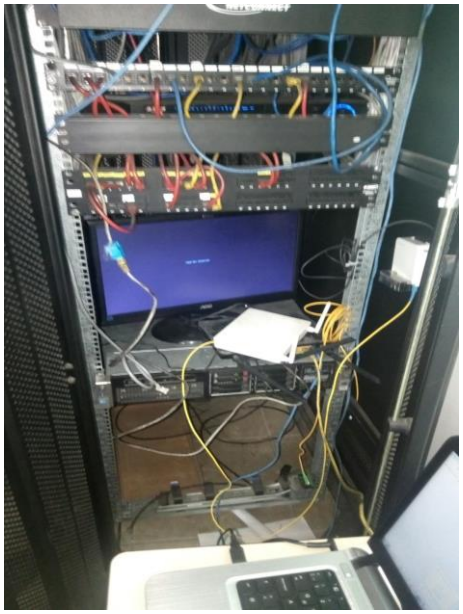
En la siguiente figura se evidencia el rack de comunicaciones. El cual esta en pésimas condiciones, ya que no cumple con las características de marquillado y organización de cables, además se observa material no permitido, como es cartón, el cual puede convertirse en un artículo que genera calor y en determinado momento fortalecer un incendio.

Figura 43. Rack de comunicaciones

Fuente: El autor

Se evidencia un monitor en el rack de comunicaciones, que es usado para observación de cámaras de seguridad, este monitoreo es una tarea específica del personal de seguridad. Además, hay mucho desorden en el rack.

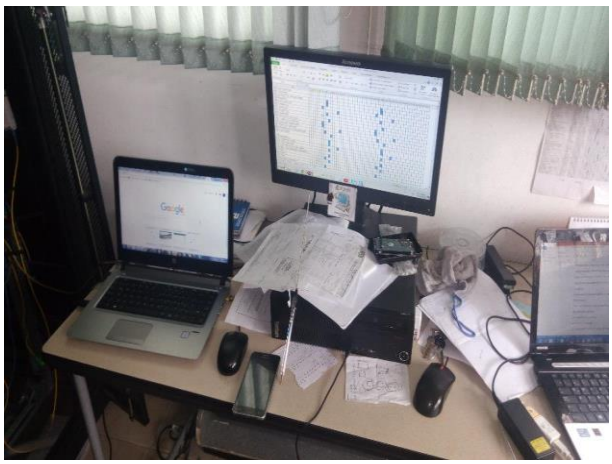
Figura 44. Monitor del servidor principal



Fuente: El autor

Se observa falta de gestión de documentos, falta de organización en el espacio de trabajo del líder de seguridad de la información.

Figura 45. Equipo de Gerencia de la información



Fuente: El autor

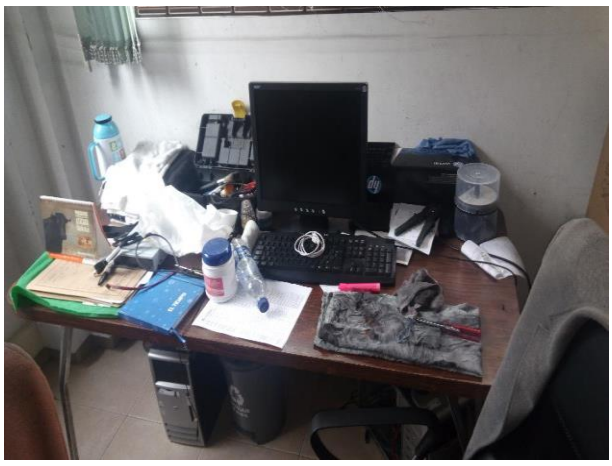
Se evidencia la UPS de 30KVA, en perfecto estado, información tomada del plan de mantenimiento. Allí se observan objetos sobre la UPS y esta debe estar totalmente libre de ellos.

Figura 46. UPS

Fuente: El autor

El espacio de trabajo del técnico de sistemas carece de orden y organización.

Figura 47. Equipo del técnico de sistemas



Fuente: El autor

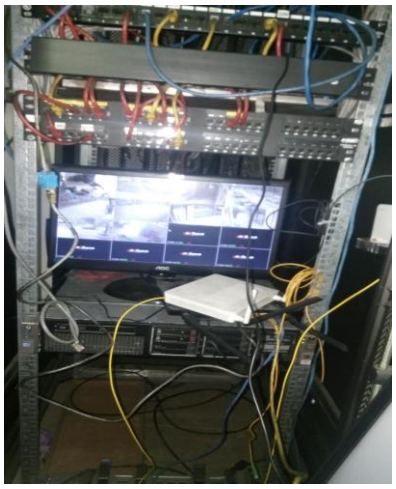
Se evidencia una torre en desuso en el piso, causando desorden.

Figura 48. Servicios de recolección mezclados con computadores

Fuente: El autor

En la parte baja del rack de comunicaciones se evidencia el monitoreo de las cámaras de seguridad de la institución, lo cual es una tarea exclusiva del personal de seguridad, pero adicionalmente se observa cierta desorganización de cables.

Figura 49. Sistema de monitoreo de cámaras de seguridad



Fuente: El autor

7.7 REVISION LISTA DE CHEQUEO ISO 27001:2013

A continuación, se describe una lista de chequeo donde se evaluará el cumplimiento de los dominios, objetivos y controles de acuerdo con la norma ISO27001:2013. Ver Anexo C.

7.8 METODOLOGÍA MAGERIT APLICADA A LA AUDITORÍA

7.8.1 Clasificación de activos

Tabla 8. Activos de Información

TIPO DE ACTIVO	ACTIVO
ACTIVO DE INFORMACION	Documentos de Normatividad Institucional
	Archivo Excel de Convenios Institucionales
	Base de datos de Contratacion del sistema de información CNT
	Base de datos de Talento humano del Sistema de Información CNT
	Base de datos de Historias Clinicas del Sistema de Información CNT
	Base de datos contable del Sistema de Información CNT
	Base de datos de Activos fijos del Sistema de Información CNT
	Base de datos de Presupuesto del Sistema de Información CNT
	Base de datos de cartera y facturación del Sistema de Información CNT
	Base de datos del servicio farmacéutico del Sistema de Información CNT
	Base de datos de Control Interno y Calidad del Sistema de Información CNT
	Base de datos de tesorería del Sistema de Información CNT
	Base de datos de Mantenimiento del Sistema de Información CNT
	Base de datos de compras y suministros del Sistema de Información CNT
SOFTWARE O APLICACIÓN	Sistema Operativo Windows 8
	Sistema Operativo Windows 7
	Sistema Operativo Windows XP
	Sistema operativo Windows Server 2012
	Software de Gestion Hospitalario CNT Systems
	Software de arquitectura Autocad 2009
	Paquete Office 2013
	Aplicativo de informes Piscis
	Aplicativo Telemedicina ITMS
HARDWARE	70 Computadores de escritorio HP
	10 Computadores portatiles HP
	1 Servidor de reportes HP
	1 Servidor de Backup HP
EQUIPAMIENTO AUXILIAR	1 Planta Industrial 100KW
	1 UPS 20 KVA
PERSONAL	1 Ingeniero de sistemas
	1 Técnico de sistemas
	150 trabajadores en diversas dependencias

Fuente: El autor

7.8.2 Tabla de convenciones

Tabla 9. Convenciones para evaluar el riesgo

VALORACIÓN DEL RIESGO								
IMPACTO	5	5	10	15	20	25		
	4	4	8	12	16	20		ZONA 1
	3	3	6	8	12	15		ZONA 2
	2	2	4	6	8	10		ZONA 3
	1	1	2	3	4	5		ZONA 4
	PROBABILIDAD							
VALORACIÓN DEL RIESGO RESIDUAL								
INACEPTABLE				> 16				
IMPORTANTE				11 a 16				
TOLERABLE				2 a 10				
ACEPTABLE				< 2				
EFICACIA DEL CONTROL								
ALTO	4							
MEDIO	3							
BAJO	2							
INEXISTENTE	1							

Fuente: El autor

7.8.3 Valoración cuantitativa de activos

A continuación, se presentan las tablas de convenciones de valoración de activos.

Tabla 10. Convenciones valoración de actvivos

VALORACION		CRITERIO
10	EXTREMO	DAÑO EXTREMADAMENTE GRAVE
9	MUY ALTO	DAÑO MUY GRAVE
6 A 8	ALTO	DAÑO GRAVE
3 A 5	MEDIO	DAÑO IMPORTANTE
1 A 2	BAJO	DAÑO MENOR
0	DESPRECIABLE	IRRELEVANTE A EFECTOS PRÁCTICOS

Fuente: El autor

A continuación, se presenta la tabla de valoración de activos

Tabla 11. Valoración de activos

VALORACIÓN DE ACTIVOS CUANTITATIVAMENTE Y CUALITATIVAMENTE					
ACTIVO	VALORACIÓN				
	D	I	C	A	T
SOFTWARE HOSPITALARIO DE MANEJO DE HISTORIAS CLINICAS ASISTENCIALES/ACTIVO DE INFORMACION	10	10	10	10	10
BASES DE DATOS GERENCIA ADMINISTRATIVA Y FINANCIERA/ACTIVO DE INFORMACION	7	7	9	9	9
BASES DE DATOS TALENTO HUMANO Y CONTRATACIÓN. //ACTIVO DE INFORMACION	8	7	9	9	9
MICROSOFT WINDOWS 7, 8, 10 Y XP/SOFTWARE	5	6	7	5	5
WINDOWS SERVER 2012/SOFTWARE	6	7	6	7	8
CNT SYSTEMS SISTEMA DE INFORMACIÓN HOSPITALARIA ASISTENCIASL Y ADMINISTRATIVA/SOFTWARE	8	7	10	8	8
MOZILLA FIREFOX Y GOOGLE CHROME (Navegadores Web) /SOFTWARE	4	3	5	5	5
MICROSOFT OFFICE 2010 (ofimática)/SOFTWARE	4	3	5	5	5
80 ESTACIONES DE TRABAJO (Portátiles y Escritorio) /HARDWARE	7	6	7	5	4
2 SERVIDORES (Datos y Reportes) /HARDWARE	7	6	7	6	4
ROUTER LINKSYS/RED	7	6	7	9	4
3 SWITCH/RED	7	6	7	9	4
CABLEADO ESTRUCTURADO/INSTALACION	7	7	9	6	8
INSTALACIÓN ELÉCTRICA (Monofásica y Trifásica) /INSTALACION	8	5	5	5	5
1 PLANTA DE ENERGÍA ELÉCTRICA Y 1 UPS 20KVA/EQUIPAMENTO AUXILIAR	10	10	5	10	10
SERVICIO DE CONEXIÓN A INTERNET/SERVICIOS	7	8	5	8	8
SERVICIOS DE MANTENIMIENTO/SERVICIOS	7	8	8	7	7
INGENIERO DE SISTEMAS/PERSONAL	7	6	6	6	6
TÉCNICO DE SISTEMAS/PERSONAL	5	5	5	5	5
150 USUARIOS/PERSONAL	5	5	5	5	5

Fuente: El autor

7.8.4 Valoración de frecuencia, impacto y riesgo potencial

Tabla 12. Valoración de frecuencia impacto y riesgo

	Activo/Amenaza	Frecuencia	Valoración impacto potencial					Valoración riesgo potencial				
			D	I	C	A	T	D	I	C	A	T
ACTIVOS DE INFORMACIÓN	**SOFTWARE HOSPITALARIO DE MANEJO DE HISTORIAS CLINICAS ASISTENCIALES/ACTIVO DE INFORMACION**											
	[N.2] Daños por agua	1	3	3				3	3			
	[I.1] Fuego	1	3	3				3	3			
	[N.*] Desastres naturales	1	3	3			2	3	3			2
	[I.4] Contaminación electromagnética	1	3	3			2	3	3			2
	[I.5] Avería de origen físico o lógico	5	5	4			2	25	20			10
	[I.6] Corte del suministro eléctrico	5	5	4			4	25	20			20
	[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9
	[E.2] Errores del administrador	2	4	4			3	8	8			6
	[E.8] Difusión de software dañino	3	4	5			4	12	15			12
	[E.15] Alteración de la información	2	5	5	5		4	10	10	10		8
	[E.16] Introducción de falsa información	2	4	4	5	5	3	8	8	10	10	6
	[E.18] Destrucción de la información	2	4	5			5	8	10			10
	[E.19] Divulgación de información	2		4	5		3		8	10		6
	[A.5] Suplantación de la identidad del usuario	3	3	5	5	5	3	9	15	15	15	9
	[A.6] Abuso de privilegios de acceso	3	3	3	3	3	2	9	9	9	9	6
	[A.8] Difusión de software dañino	2	4	5			4	8	10			8
	[A.11] Acceso no autorizado	2	3	3	5	3		6	6	10	6	

Tabla 13. (Continuación)

[A.15] Modificación de información	3	4	4	5	5	4	12	12	15	15	12
[A.16] Introducción de falsa información	2	4	4	5	5	3	8	8	10	10	6
BASES DE DATOS GERENCIA ADMINISTRATIVA Y FINANCIERA/ACTIVO DE INFORMACION											
[N.*] Desastres naturales	1	3	3				3	3			
[I.1] Fuego	1	3	3				3	3			
[I.2] Daños por agua	1	3	3				3	3			
[I.*] Desastres industriales	1	3	3				3	3			
[I.4] Contaminación electromagnética	1	5	4				5	4			
[I.6] Corte del suministro eléctrico	5	5	4			4	25	20			20
[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9
[E.2] Errores del administrador	3	4	4			3	12	12			9
[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4
[E.16] Introducción de falsa información	2	4	4	5	5	3	8	8	10	10	6
[E.18] Destrucción de la información	1	4	5			5	4	5			5
[E.19] Divulgación de información	3		4	5		3		12	15		9
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	4	4			3	8	8			6
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9
[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6

Tabla 13. (Continuación)

[A.6] Abuso de privilegios de acceso	3	3	3	3	3	2	9	9	9	9	6
[A.8] Difusión de software dañino	2	4	5			4	8	10			8
[A.11] Acceso no autorizado	2		5	5	5			10	10	10	
[A.15] Modificación de información	3	4	4	5	5	4	12	12	15	15	12
[A.16] Introducción de falsa información	2	4	4	5	5	3	8	8	10	10	6
[A.17] Corrupción de la información	2		5	5	3	3		10	10	6	6
[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4
[A.19] Divulgación de información	4		4	5		3		16	20		12
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4
[A.26] Ataque destructivo	1	5	5				5	5			
BASES DE DATOS TALENTO HUMANO Y CONTRATACIÓN.//ACTIVO DE INFORMACION											
[N.*] Desastres naturales	1	3	3				3	3			
[I.1] Fuego	1	3	3				3	3			
[I.2] Daños por agua	1	3	3			2	3	3			2
[I.*] Desastres industriales	1	3	3			2	3	3			2
[I.4] Contaminación electromagnética	1	2	2			1	2	2			1
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12
[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
[E.1] Errores de los usuarios	1	4	4	4		3	4	4	4		3
[E.2] Errores del administrador	1	4	4			3	4	4			3
[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4
[E.16] Introducción de falsa información	1	4	4	5	5	3	4	4	5	5	3
[E.18] Destrucción de la información	1	4	5			5	4	5			5
[E.19] Divulgación de información	2		4	5		3		8	10		6

Tabla 13. (Continuación)

	[E.21] Errores de mantenimiento / actualización de programas (software)	1	4	4			3	4	4			3
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	5	4			4	5	4			4
	[E.24] Caída del sistema por agotamiento de recursos	1	3	3			3	3	3			3
	[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5
	[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
	[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
	[A.8] Difusión de software dañino	2	4	5			4	8	10			8
	[A.11] Acceso no autorizado	2		5	5	5			10	10	10	
	[A.14] Interceptación de información (escucha)	2		5	5	5	4		10	10	10	8
	[A.15] Modificación de información	2	4	4	5	5	4	8	8	10	10	8
	[A.16] Introducción de falsa información	2	4	4	5	5	3	8	8	10	10	6
	[A.17] Corrupción de la información	2		5	5	3	3		10	10	6	6
	[A.18] Destrucción de la información	2	5	5	4		4	10	10	8		8
	[A.19] Divulgación de información	3		4	5				12	15		
	[A.25] Robo de equipos	2	4	4	4		4	8	8	8		8
	[A.26] Ataque destructivo	2	5	5				10	10			
ACTIVOS DE SOFTWARE	**MICROSOFT WINDOWS 7, 8, 10 Y XP/SOFTWARE**											
	[I.4] Contaminación electromagnética	1	4	4			4	4	4			4
	[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
	[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12
	[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9

Tabla 13. (Continuación)

[E.2] Errores del administrador	3	4	4			3	12	12			9
[E.4] Errores de configuración	2	4	4		4	4	8	8		8	8
[E.8] Difusión de software dañino	2	4	5			4	8	10			8
[E.20] Vulnerabilidades de los programas (software)	2	4	4		4	4	8	8		8	8
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
[A.8] Difusión de software dañino	3	4	5			4	12	15			12
[A.11] Acceso no autorizado	2		4	4	4			8	8	8	
[A.13] Repudio	2	4				3	8				6
[A.22] Manipulación de programas	3	3	4	3	4	3	9	12	9	12	9
[A.24] Denegación de servicio	1	4	4			3	4	4			3
[A.28] Indisponibilidad del personal	3	3				4	9				12
WINDOWS SERVER 2012/SOFTWARE											
[I.4] Contaminación electromagnética	1	4	4			4	4	4			4
[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9
[E.2] Errores del administrador	3	4	4			3	12	12			9
[E.4] Errores de configuración	2	4	3			3	8	6			6

Tabla 13. (Continuación)

	[E.8] Difusión de software dañino	2	4	4				8	8			
	[E.20] Vulnerabilidades de los programas (software)	2	4	5	5		3	8	10	10		6
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6
	[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9
	[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6
	[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9
	[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
	[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
	[A.8] Difusión de software dañino	3	4	5			4	12	15			12
	[A.11] Acceso no autorizado	2		4	4	4			8	8	8	
	[A.13] Repudio	2	5				4	10				8
	[A.22] Manipulación de programas	3	3	4	3	4	3	9	12	9	12	9
	[A.24] Denegación de servicio	1	4	4			3	4	4			3
	[A.28] Indisponibilidad del personal	4	3				4	12				16
	CNT SYSTEMS SISTEMA DE INFORMACIÓN HOSPITALARIA ASISTENCIASL Y ADMINISTRATIVA/SOFTWARE											
	[I.4] Contaminación electromagnética	1	4	4			4	4	4			4
	[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
	[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12
	[I.11] Emanaciones electromagnéticas	1										
	[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9

Tabla 13. (Continuación)

[E.2] Errores del administrador	3	4	4			3	12	12			9
[E.4] Errores de configuración	2	4	3			3	8	6			6
[E.8] Difusión de software dañino	2	4	4				8	8			
[E.20] Vulnerabilidades de los programas (software)	2	4	5	5		3	8	10	10		6
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
[A.8] Difusión de software dañino	3	4	5			4	12	15			12
[A.11] Acceso no autorizado	2		5	5	5	2		10	10	10	4
[A.13] Repudio	2	5				5	10				10
[A.22] Manipulación de programas	3	5	5	5	4	3	15	15	15	12	9
[A.24] Denegación de servicio	1	5	4			3	5	4			3
[A.28] Indisponibilidad del personal	4	4				4	16				16
MOZILLA FIREFOX Y GOOGLE CHROME (Navegadores Web)/SOFTWARE											
[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9
[E.2] Errores del administrador	3	4	4			3	12	12			9

Tabla 13. (Continuación)

	[E.4] Errores de configuración	2	4	3			3	8	6			6
	[E.8] Difusión de software dañino	2	4	4				8	8			
	[E.20] Vulnerabilidades de los programas (software)	2	4	5	5		3	8	10	10		6
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6
	[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9
	[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6
	[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9
	[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
	[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
	[A.8] Difusión de software dañino	3	4	5			4	12	15			12
	[A.11] Acceso no autorizado	2		3	3	3			6	6	6	
	[A.13] Repudio	2	3				3	6				6
	[A.24] Denegación de servicio	1	3	3			3	3	3			3
	[A.28] Indisponibilidad del personal	3	4				4	12				12
	MICROSOFT OFFICE 2010 (ofimática)/SOFTWARE											
	[I.4] Contaminación electromagnética	1	4	4			4	4	4			4
	[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
	[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12
	[I.11] Emanaciones electromagnéticas	1	4	4			4	4	4			4
	[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9
	[E.2] Errores del administrador	3	4	4			3	12	12			9
	[E.4] Errores de configuración	2	4	3			3	8	6			6
	[E.8] Difusión de software dañino	2	4	4				8	8			

Tabla 13. (Continuación)

	[E.20] Vulnerabilidades de los programas (software)	2	4	5	5		3	8	10	10		6
	[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6
	[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9
	[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6
	[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9
	[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
	[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
	[A.8] Difusión de software dañino	3	4	5			4	12	15			12
	[A.11] Acceso no autorizado	2		3	3	3			6	6	6	
	[A.13] Repudio	2	2				2	4				4
	[A.22] Manipulación de programas	3	3	4	3	4	3	9	12	9	12	9
	[A.24] Denegación de servicio	1	4	4			3	4	4			3
	[A.28] Indisponibilidad del personal	2	4				4	8				8
ACTIVOS DE HARDWARE	**80 ESTACIONES DE TRABAJO (Portátiles y Escritorio)/HARDWARE**											
	[N.1] Fuego	1	4	4			4	4	4			4
	[N.2] Daños por agua	1	4	4			4	4	4			4
	[N.*] Desastres naturales	1	4	4			4	4	4			4
	[I.1] Fuego	1	4	4			4	4	4			4
	[I.2] Daños por agua	1	4	4			4	4	4			4
	[I.*] Desastres industriales	1	4	4			4	4	4			4
	[I.3] Contaminación mecánica	1	4	4			4	4	4			4
	[I.4] Contaminación electromagnética	2	4	4			4	8	8			8
	[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
	[I.6] Corte del suministro eléctrico	5	5	4			4	25	20			20

Tabla 13. (Continuación)

[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	4			4	10	8			8
[I.8] Fallo de servicios de comunicacioneS	3	5	4			4	15	12			12
[I.9] Interrupción de otros servicios o suministros esenciales	2	5	4			4	10	8			8
[I.11] Emanaciones electromagnéticas	2	4	4			4	8	8			8
[E.24] Caída delsistema por agotamiento de recursos	3	3	3			3	9	9			9
[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
[A.7] Uso no previsto	2					4					8
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4
[A.26] Ataque destructivo	2	5	5			3	10	10			6
[A.27] Ocupación enemiga	1	5	5			4	5	5			4
[A.28] Indisponibilidad del personal	2	4				4	8				8
2 SERVIDORES (Datos y Reportes)/HARDWARE											
[N.1] Fuego	1	4	4			4	4	4			4
[N.2] Daños por agua	1	4	4			4	4	4			4
[N.*] Desastres naturales	1	4	4			4	4	4			4
[I.1] Fuego	1	4	4			4	4	4			4
[I.2] Daños por agua	1	4	4			4	4	4			4
[I.*] Desastres industriales	1	4	4			4	4	4			4
[I.3] Contaminación mecánica	1	4	4			4	4	4			4
[I.4] Contaminación electromagnética	2	4	4			4	8	8			8
[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
[I.6] Corte del suministro eléctrico	5	5	4			4	25	20			20

Tabla 13. (Continuación)

	[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	4			4	10	8			8
	[I.8] Fallo de servicios de comunicacioneS	3	5	4			4	15	12			12
	[I.9] Interrupción de otros servicios o suministros esenciales	2	5	4			4	10	8			8
	[I.11] Emanaciones electromagnéticas	2	4	4			4	8	8			8
	[E.24] Caída delsistema por agotamiento de recursos	3	3	3			3	9	9			9
	[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5
	[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6
	[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9
	[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
	[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
	[A.7] Uso no previsto	2					4					8
	[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4
	[A.26] Ataque destructivo	2	5	5			3	10	10			6
	[A.27] Ocupación enemiga	1	5	5			4	5	5			4
	[A.28] Indisponibilidad del personal	2	4				4	8				8
ACTIVOS DE RED	**ROUTER LINKSYS/RED**											
	[N.1] Fuego	1	4	4			4	4	4			4
	[N.2] Daños por agua	1	4	4			4	4	4			4
	[N.*] Desastres naturales	1	4	4			4	4	4			4
	[I.1] Fuego	1	4	4			4	4	4			4
	[I.2] Daños por agua	1	4	4			4	4	4			4
	[I.*] Desastres industriales	1	4	4			4	4	4			4
	[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
	[I.6] Corte del suministro eléctrico	5	5	4			4	25	20			20
	[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	4			4	10	8			8
	[E.1] Errores de los usuarios	2	4	4	4		3	8	8	8		6

Tabla 13. (Continuación)

	[E.4] Errores de configuración	2	4	3			3	8	6			6
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	5	4			4	10	8			8
	[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5
	[A.4] Manipulación de la configuración	2	5	5	4	5	3	10	10	8	10	6
	[A.6] Abuso de privilegios de acceso	1	3	3	3	3	2	3	3	3	3	2
	[A.11] Acceso no autorizado	1	3	3	5	3		3	3	5	3	
	[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4
	[A.26] Ataque destructivo	1	5	5			3	5	5			3
	[A.28] Indisponibilidad del personal	2	4				4	8				8
	3 SWITCH/RED											
	[N.1] Fuego	1	4	4			4	4	4			4
	[N.2] Daños por agua	1	4	4			4	4	4			4
	[N.*] Desastres naturales	1	4	4			4	4	4			4
	[I.1] Fuego	1	4	4			4	4	4			4
	[I.2] Daños por agua	1	4	4			4	4	4			4
	[I.*] Desastres industriales	1	4	4			4	4	4			4
	[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
	[I.6] Corte del suministro eléctrico	5	5	4			4	25	20			20
	[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	4			4	10	8			8
	[E.4] Errores de configuración	1	4	3			3	4	3			3
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	5	4			4	5	4			4
	[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5
	[A.4] Manipulación de la configuración	1	5	5	4	5	3	5	5	4	5	3
	[A.6] Abuso de privilegios de acceso	1	3	3	3	3	2	3	3	3	3	2
	[A.11] Acceso no autorizado	1	3	3	5	3		3	3	5	3	
	[A.26] Ataque destructivo	1	5	5			3	5	5			3

Tabla 13. (Continuación)

	[A.28] Indisponibilidad del personal	1	4				4	4				4
ACTIVOS DE INSTALACIÓN	**CABLEADO ESTRUCTURADO/INSTALACION**											
	[N.1] Fuego	1	4	4			4	4	4			4
	[N.2] Daños por agua	1	4	4			4	4	4			4
	[N.*] Desastres naturales	1	4	4			4	4	4			4
	[I.1] Fuego	1	4	4			4	4	4			4
	[I.2] Daños por agua	1	4	4			4	4	4			4
	[I.*] Desastres industriales	1	4	4			4	4	4			4
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4
	[E.1] Errores de los usuarios	1	4	4	4		3	4	4	4		3
	[A.26] Ataque destructivo	1	5	5			3	5	5			3
	[A.28] Indisponibilidad del personal	1	4				4	4				4
	INSTALACIÓN ELÉCTRICA (Monofásica y Trifásica)/INSTALACION											
	[N.1] Fuego	1	4	4			4	4	4			4
	[N.2] Daños por agua	1	4	4			4	4	4			4
	[N.*] Desastres naturales	1	4	4			4	4	4			4
	[I.1] Fuego	1	4	4			4	4	4			4
	[I.2] Daños por agua	1	4	4			4	4	4			4
	[I.*] Desastres industriales	1	4	4			4	4	4			4
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4
	[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9
	[A.26] Ataque destructivo	1	5	5			3	5	5			3
	[A.28] Indisponibilidad del personal	1	4				4	4				4
ACTIVOS DE	**1 PLANTA DE ENERGÍA ELÉCTRICA Y 1 UPS 20KVA/EQUIPAMENTO AUXILIAR**											
	[N.1] Fuego	1	4	4			4	4	4			4
	[N.2] Daños por agua	1	4	4			4	4	4			4
	[N.*] Desastres naturales	1	4	4			4	4	4			4

Tabla 13. (Continuación)

	[I.1] Fuego	1	4	4			4	4	4			4
	[I.2] Daños por agua	1	4	4			4	4	4			4
	[I.*] Desastres industriales	1	4	4			4	4	4			4
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4
	[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9
	[A.26] Ataque destructivo	1	5	5			3	5	5			3
	[A.28] Indisponibilidad del personal	1	4				4	4				4
ACTIVOS DE SERVICIOS	**SERVICIO DE CONEXIÓN A INTERNET/SERVICIOS**											
	[N.1] Fuego	1	4	4			4	4	4			4
	[N.2] Daños por agua	1	4	4			4	4	4			4
	[N.*] Desastres naturales	1	4	4			4	4	4			4
	[I.1] Fuego	1	4	4			4	4	4			4
	[I.2] Daños por agua	1	4	4			4	4	4			4
	[I.*] Desastres industriales	1	4	4			4	4	4			4
	[I.4] Contaminación electromagnética	1	4	4			4	4	4			4
	[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8
	[I.6] Corte del suministro eléctrico	5	5	4			4	25	20			20
	[I.8] Fallo de servicios de comunicaciones	5	5	4			4	25	20			20
	[E.1] Errores de los usuarios	2	4	4	4		3	8	8	8		6
	[E.2] Errores del administrador	1	4	4			3	4	4			3
	[E.4] Errores de configuración	2	4	3			3	8	6			6
	[E.8] Difusión de software dañino	1	4	4				4	4			
	[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9
	[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5
	[E.28] Indisponibilidad del personal	1	3	3			3	3	3			3
	[A.4] Manipulación de la configuración	1	5	5	4	5	3	5	5	4	5	3
	[A.12] Análisis de tráfico	1	2	2			2	2	2			2
	[A.13] Repudio	1	4				3	4				3

Tabla 13. (Continuación)

[A.14] Interceptación de información (escucha)	1		4	4	4	4		4	4	4	4
[A.16] Introducción de falsa información	1	4	4	5	5	3	4	4	5	5	3
[A.24] Denegación de servicio	1	4	4			3	4	4			3
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4
[A.26] Ataque destructivo	1	5	5			3	5	5			3
SERVICIOS DE MANTENIMIENTO/SERVICIOS											
[N.1] Fuego	1	4	4			4	4	4			4
[N.2] Daños por agua	1	4	4			4	4	4			4
[N.*] Desastres naturales	1	4	4			4	4	4			4
[I.1] Fuego	1	4	4			4	4	4			4
[I.2] Daños por agua	1	4	4			4	4	4			4
[I.*] Desastres industriales	1	4	4			4	4	4			4
[I.5] Avería de origen físico o lógico	5	4	4			4	20	20			20
[I.6] Corte del suministro eléctrico	5	5	4			4	25	20			20
[I.8] Fallo de servicios de comunicaciones	2	5	4			4	10	8			8
[E.1] Errores de los usuarios	2	4	4	4		3	8	8	8		6
[E.2] Errores del administrador	2	4	4			3	8	8			6
[E.4] Errores de configuración	1	4	3			3	4	3			3
[E.8] Difusión de software dañino	1	4	4				4	4			
[E.28] Indisponibilidad del personal	1	3	3			3	3	3			3
[A.4] Manipulación de la configuración	2	5	5	4	5	3	10	10	8	10	6
[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
[A.17] Corrupción de la información	1		5	5	4	4		5	5	4	4
[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4
[A.19] Divulgación de información	2		4	5				8	10		
[A.24] Denegación de servicio	1	4	4			3	4	4			3
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4

Tabla 13. (Continuación)

	[A.26] Ataque destructivo	1	5	5			3	5	5			3
ACTIVOS DE RECURSO HUMANO	**INGENIERO DE SISTEMAS/PERSONAL**											
	[N.1] Fuego	1	4	4			4	4	4			4
	[N.2] Daños por agua	1	4	4			4	4	4			4
	[N.*] Desastres naturales	1	4	4			4	4	4			4
	[I.1] Fuego	1	4	4			4	4	4			4
	[I.*] Desastres industriales	1	4	4			4	4	4			4
	[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4
	[I.8] Fallo de servicios de comunicaciones	2	5	4			4	10	8			8
	[E.7] Deficiencias en la organización	2					4					8
	[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4
	[E.16] Introducción de falsa información	1	5	5	5		4	5	5	5		4
	[E.18] Destrucción de la información	1	4	5			5	4	5			5
	[E.19] Divulgación de información	2		4	5		3		8	10		6
	[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6
	[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
	[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
	[A.17] Corrupción de la información	1		5	5	4	4		5	5	4	4
	[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4
	[A.19] Divulgación de información	5		4	5				20	25		
	[A.28] Indisponibilidad del personal	3	4				4	12				12
	[A.30] Ingeniería social (picaresca)	5		5	5		4		25	25		20
	TÉCNICO DE SISTEMAS/PERSONAL											
	[N.1] Fuego	1	4	4			4	4	4			4
	[N.2] Daños por agua	1	4	4			4	4	4			4

Tabla 13. (Continuación)

[N.*] Desastres naturales	1	4	4			4	4	4			4
[I.1] Fuego	1	4	4			4	4	4			4
[I.*] Desastres industriales	1	4	4			4	4	4			4
[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4
[I.8] Fallo de servicios de comunicaciones	2	5	4			4	10	8			8
[E.7] Deficiencias en la organización	2					4					8
[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4
[E.16] Introducción de falsa información	1	5	5	5		4	5	5	5		4
[E.18] Destrucción de la información	1	4	5			5	4	5			5
[E.19] Divulgación de información	2		4	5		3		8	10		6
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
[A.17] Corrupción de la información	1		5	5	4	4		5	5	4	4
[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4
[A.19] Divulgación de información	5		4	5				20	25		
[A.28] Indisponibilidad del personal	3	4				4	12				12
[A.30] Ingeniería social (picaresca)	5		5	5		4		25	25		20
150 USUARIOS/PERSONAL											
[N.1] Fuego	1	4	4			4	4	4			4
[N.2] Daños por agua	1	4	4			4	4	4			4
[N.*] Desastres naturales	1	4	4			4	4	4			4
[I.1] Fuego	1	4	4			4	4	4			4
[I.*] Desastres industriales	1	4	4			4	4	4			4
[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4

Tabla 13. (Continuación)

	[I.8] Fallo de servicios de comunicaciones	3	5	4			4	15	12			12
	[E.7] Deficiencias en la organización	2					4					8
	[E.15] Alteración de la información	2	5	5	5		4	10	10	10		8
	[E.16] Introducción de falsa información	2	5	5	5		4	10	10	10		8
	[E.18] Destrucción de la información	1	4	5			5	4	5			5
	[E.19] Divulgación de información	2		5	5		3		10	10		6
	[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6
	[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6
	[A.6] Abuso de privilegios de acceso	2	3	3	3	3	2	6	6	6	6	4
	[A.17] Corrupción de la información	2		5	5	4	4		10	10	8	8
	[A.18] Destrucción de la información	1	5	5	4		5	5	5	4		5
	[A.19] Divulgación de información	5		4	5				20	25		
	[A.28] Indisponibilidad del personal	5	4				4	20				20
	[A.30] Ingeniería social (picaresca)	5		5	5		4		25	25		20

Fuente: El autor

7.8.5 Aplicación de controles y análisis de riesgo residual

Tabla 13. Aplicación de controles

	Activo/Amenaza	Controles ISO 27001-27002:2013	Eficacia de control	Valoración riesgo residual				
				D	I	C	A	T
ACTIVOS DE INFORMACIÓN	**SOFTWARE HOSPITALARIO DE MANEJO DE HISTORIAS CLINICAS ASISTENCIALES/ACTIVO DE INFORMACION**							
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,0	1,0	0,0	0,0	0,0
	[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5	0,0	0,0	0,0
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,0	1,0	0,0	0,0	0,7
	[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,0	1,0	0,0	0,0	0,7
	[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	6,3	5,0	0,0	0,0	2,5
	[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	6,3	5,0	0,0	0,0	5,0
	[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0	0,0	3,0
	[E.2] Errores del administrador	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	2,0	2,0	0,0	0,0	1,5
	[E.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	3,0	3,8	0,0	0,0	3,0
	[E.15] Alteración de la información	9.4.1 Restricción del acceso a la información.	4	2,5	2,5	2,5	0,0	2,0
	[E.16] Introducción de falsa información	9.4.1 Restricción del acceso a la información.	4	2,0	2,0	2,5	2,5	1,5
	[E.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	3	2,7	3,3	0,0	0,0	3,3
	[E.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	3	0,0	2,7	3,3	0,0	2,0
	[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	2,3	3,8	3,8	3,8	2,3

Tabla 14. (Continuación)

[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	3,0	3,0	3,0	3,0	2,0
[A.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	2,0	2,5	0,0	0,0	2,0
[A.11] Acceso no autorizado	9.1.1 Política de control de accesos.	4	1,5	1,5	2,5	1,5	0,0
[A.15] Modificación de información	9.4.1 Restricción del acceso a la información.	4	3,0	3,0	3,8	3,8	3,0
[A.16] Introducción de falsa información	9.4.1 Restricción del acceso a la información.	4	2,0	2,0	2,5	2,5	1,5
BASES DE DATOS GERENCIA ADMINISTRATIVA Y FINANCIERA/ACTIVO DE INFORMACION							
[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,0	1,0	0,0	0,0	0,0
[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5	0,0	0,0	0,0
[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5	0,0	0,0	0,0
[I.*] Desastres industriales	16.1.2 Notificación de los eventos de seguridad de la información.	2	1,5	1,5	0,0	0,0	0,0
[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3	0,0	0,0	0,0
[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	6,3	5,0	0,0	0,0	5,0
[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0
[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0	0,0	3,0
[E.2] Errores del administrador	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0	0,0	0,0	2,3
[E.15] Alteración de la información	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3	0,0	1,0
[E.16] Introducción de falsa información	9.4.1 Restricción del acceso a la información.	4	2,0	2,0	2,5	2,5	1,5
[E.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	3	1,3	1,7	0,0	0,0	1,7
[E.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	3	0,0	4,0	5,0	0,0	3,0

Tabla 14. (Continuación)

	[E.21] Errores de mantenimiento / actualización de programas (software)	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0	0,0	0,0	1,5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	14.2.2 Procedimientos de control de cambios en los sistemas.	4	2,0	2,0	0,0	0,0	1,5
	[E.24] Caída del sistema por agotamiento de recursos	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0	0,0	0,0	3,0
	[E.25] Pérdida de equipos	8.1.1 Inventario de activos.	4	1,3	1,3	1,3	0,0	1,3
	[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
	[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	3,0	3,0	3,0	3,0	2,0
	[A.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	2,0	2,5	0,0	0,0	2,0
	[A.11] Acceso no autorizado	9.1.1 Política de control de accesos.	4	0,0	2,5	2,5	2,5	0,0
	[A.15] Modificación de información	9.4.1 Restricción del acceso a la información.	4	3,0	3,0	3,8	3,8	3,0
	[A.16] Introducción de falsa información	9.4.1 Restricción del acceso a la información.	4	2,0	2,0	2,5	2,5	1,5
	[A.17] Corrupción de la información	8.2.2 Etiquetado y manipulado de la información.	3	0,0	3,3	3,3	2,0	2,0
	[A.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0	0,0	1,0
	[A.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	4	0,0	4,0	5,0	0,0	3,0
	[A.25] Robo de equipos	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0	0,0	1,0
	[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	0,0	0,0	0,0
	BASES DE DATOS TALENTO HUMANO Y CONTRATACIÓN.//ACTIVO DE INFORMACION							
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,0	1,0	0,0	0,0	0,0
	[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5	0,0	0,0	0,0
	[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5	0,0	0,0	1,0

Tabla 14. (Continuación)

[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5	0,0	0,0	1,0
[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales.	3	0,7	0,7	0,0	0,0	0,3
[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0	0,0	0,0	3,0
[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0
[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	1,3	1,3	1,3	0,0	1,0
[E.2] Errores del administrador	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	1,0	1,0	0,0	0,0	0,8
[E.15] Alteración de la información	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3	0,0	1,0
[E.16] Introducción de falsa información	9.4.1 Restricción del acceso a la información.	4	1,0	1,0	1,3	1,3	0,8
[E.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	3	1,3	1,7	0,0	0,0	1,7
[E.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	3	0,0	2,7	3,3	0,0	2,0
[E.21] Errores de mantenimiento / actualización de programas (software)	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	1,0	1,0	0,0	0,0	0,8
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	14.2.2 Procedimientos de control de cambios en los sistemas.	4	1,3	1,0	0,0	0,0	1,0
[E.24] Caída del sistema por agotamiento de recursos	11.2.4 Mantenimiento de los equipos.	3	1,0	1,0	0,0	0,0	1,0
[E.25] Pérdida de equipos	8.1.1 Inventario de activos.	4	1,3	1,3	1,3	0,0	1,3
[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
[A.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	2,0	2,5	0,0	0,0	2,0
[A.11] Acceso no autorizado	9.1.1 Política de control de accesos.	4	0,0	2,5	2,5	2,5	0,0
[A.14] Interceptación de información (escucha)	9.2.4 Gestión de información confidencial de autenticación de usuarios.	3	0,0	3,3	3,3	3,3	2,7

Tabla 14. (Continuación)

	[A.15] Modificación de información	9.4.1 Restricción del acceso a la información.	4	2,0	2,0	2,5	2,5	2,0
	[A.16] Introducción de falsa información	9.4.1 Restricción del acceso a la información.	4	2,0	2,0	2,5	2,5	1,5
	[A.17] Corrupción de la información	8.2.2 Etiquetado y manipulado de la información.	3	0,0	3,3	3,3	2,0	2,0
	[A.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	4	2,5	2,5	2,0	0,0	2,0
	[A.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	4	0,0	3,0	3,8	0,0	0,0
	[A.25] Robo de equipos	11.1.3 Seguridad de oficinas, despachos y recursos.	4	2,0	2,0	2,0	0,0	2,0
	[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	2,5	2,5	0,0	0,0	0,0
ACTIVOS DE SOFTWARE	**MICROSOFT WINDOWS 7, 8, 10 Y XP/SOFTWARE**							
	[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0
	[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0	0,0	0,0	3,0
	[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0	0,0	3,0
	[E.2] Errores del administrador	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0	0,0	0,0	2,3
	[E.4] Errores de configuración	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0	0,0	2,0	2,0
	[E.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	2,0	2,5	0,0	0,0	2,0
	[E.20] Vulnerabilidades de los programas (software)	14.2.9 Pruebas de aceptación.	3	2,7	2,7	0,0	2,7	2,7
	[E.21] Errores de mantenimiento / actualización de programas (software)	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0	0,0	0,0	1,5
	[E.24] Caída del sistema por agotamiento de recursos	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0	0,0	0,0	3,0
	[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0	0,0	0,0	2,0

Tabla 14. (Continuación)

	[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	5,0	5,0	4,0	5,0	3,0
	[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
	[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
	[A.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	3,0	3,8	0,0	0,0	3,0
	[A.11] Acceso no autorizado	9.1.1 Política de control de accesos.	4	0,0	2,0	2,0	2,0	0,0
	[A.13] Repudio	9.1.2 Control de acceso a las redes y servicios asociados.	3	2,7	0,0	0,0	0,0	2,0
	[A.22] Manipulación de programas	9.4.4 Uso de herramientas de administración de sistemas.	4	2,3	3,0	2,3	3,0	2,3
	[A.24] Denegación de servicio	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0	0,0	0,0	0,8
	[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	9,0	0,0	0,0	0,0	12,0
	WINDOWS SERVER 2012/SOFTWARE							
	[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0
	[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0	0,0	0,0	3,0
	[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0	0,0	3,0
	[E.2] Errores del administrador	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0	0,0	0,0	2,3
	[E.4] Errores de configuración	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5	0,0	0,0	1,5
	[E.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	2,0	2,0	0,0	0,0	0,0
	[E.20] Vulnerabilidades de los programas (software)	14.2.9 Pruebas de aceptación.	3	2,7	3,3	3,3	0,0	2,0
	[E.21] Errores de mantenimiento / actualización de programas (software)	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0	0,0	0,0	1,5

Tabla 14. (Continuación)

	[E.24] Caída del sistema por agotamiento de recursos	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0	0,0	0,0	3,0
	[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0	0,0	0,0	2,0
	[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	5,0	5,0	4,0	5,0	3,0
	[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
	[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
	[A.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	3,0	3,8	0,0	0,0	3,0
	[A.11] Acceso no autorizado	9.1.1 Política de control de accesos.	4	0,0	2,0	2,0	2,0	0,0
	[A.13] Repudio	9.1.2 Control de acceso a las redes y servicios asociados.	3	3,3	0,0	0,0	0,0	2,7
	[A.22] Manipulación de programas	9.4.4 Uso de herramientas de administración de sistemas.	4	2,3	3,0	2,3	3,0	2,3
	[A.24] Denegación de servicio	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0	0,0	0,0	0,8
	[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	12,0	0,0	0,0	0,0	16,0
	CNT SYSTEMS SISTEMA DE INFORMACIÓN HOSPITALARIA ASISTENCIASL Y ADMINISTRATIVA/SOFTWARE							
	[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0
	[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0	0,0	0,0	3,0
	[I.11] Emanaciones electromagnéticas	11.1.4 Protección contra las amenazas externas y ambientales.	2	0,0	0,0	0,0	0,0	0,0
	[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0	0,0	3,0

Tabla 14. (Continuación)

[E.2] Errores del administrador	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0	0,0	0,0	2,3
[E.4] Errores de configuración	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5	0,0	0,0	1,5
[E.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	2,0	2,0	0,0	0,0	0,0
[E.20] Vulnerabilidades de los programas (software)	14.2.9 Pruebas de aceptación.	3	2,7	3,3	3,3	0,0	2,0
[E.21] Errores de mantenimiento / actualización de programas (software)	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0	0,0	0,0	1,5
[E.24] Caída del sistema por agotamiento de recursos	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0	0,0	0,0	3,0
[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0	0,0	0,0	2,0
[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	5,0	5,0	4,0	5,0	3,0
[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
[A.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	3,0	3,8	0,0	0,0	3,0
[A.11] Acceso no autorizado	9.1.1 Política de control de accesos.	4	0,0	2,5	2,5	2,5	1,0
[A.13] Repudio	9.1.2 Control de acceso a las redes y servicios asociados.	3	3,3	0,0	0,0	0,0	3,3
[A.22] Manipulación de programas	9.4.4 Uso de herramientas de administración de sistemas.	4	3,8	3,8	3,8	3,0	2,3
[A.24] Denegación de servicio	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,3	1,0	0,0	0,0	0,8
[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	16,0	0,0	0,0	0,0	16,0
MOZILLA FIREFOX Y GOOGLE CHROME (Navegadores Web)/SOFTWARE							
[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0

Tabla 14. (Continuación)

[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0	0,0	0,0	3,0
[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0	0,0	3,0
[E.2] Errores del administrador	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0	0,0	0,0	2,3
[E.4] Errores de configuración	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5	0,0	0,0	1,5
[E.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	2,0	2,0	0,0	0,0	0,0
[E.20] Vulnerabilidades de los programas (software)	14.2.9 Pruebas de aceptación.	3	2,7	3,3	3,3	0,0	2,0
[E.21] Errores de mantenimiento / actualización de programas (software)	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0	0,0	0,0	1,5
[E.24] Caída del sistema por agotamiento de recursos	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0	0,0	0,0	3,0
[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0	0,0	0,0	2,0
[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	5,0	5,0	4,0	5,0	3,0
[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
[A.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	3,0	3,8	0,0	0,0	3,0
[A.11] Acceso no autorizado	9.1.1 Política de control de accesos.	4	0,0	1,5	1,5	1,5	0,0
[A.13] Repudio	9.1.2 Control de acceso a las redes y servicios asociados.	3	2,0	0,0	0,0	0,0	2,0
[A.24] Denegación de servicio	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	0,8	0,8	0,0	0,0	0,8
[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	12,0	0,0	0,0	0,0	12,0
MICROSOFT OFFICE 2010 (ofimática)/SOFTWARE							

Tabla 14. (Continuación)

[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0
[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0	0,0	0,0	3,0
[I.11] Emanaciones electromagnéticas	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0	0,0	3,0
[E.2] Errores del administrador	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0	0,0	0,0	2,3
[E.4] Errores de configuración	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5	0,0	0,0	1,5
[E.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	2,0	2,0	0,0	0,0	0,0
[E.20] Vulnerabilidades de los programas (software)	14.2.9 Pruebas de aceptación.	3	2,7	3,3	3,3	0,0	2,0
[E.21] Errores de mantenimiento / actualización de programas (software)	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0	0,0	0,0	1,5
[E.24] Caída del sistema por agotamiento de recursos	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0	0,0	0,0	3,0
[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0	0,0	0,0	2,0
[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	5,0	5,0	4,0	5,0	3,0
[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
[A.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	3,0	3,8	0,0	0,0	3,0
[A.11] Acceso no autorizado	9.1.1 Política de control de accesos.	4	0,0	1,5	1,5	1,5	0,0
[A.13] Repudio	9.1.2 Control de acceso a las redes y servicios asociados.	3	1,3	0,0	0,0	0,0	1,3
[A.22] Manipulación de programas	9.4.4 Uso de herramientas de administración de sistemas.	4	2,3	3,0	2,3	3,0	2,3

Tabla 14. (Continuación)

	[A.24] Denegación de servicio	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0	0,0	0,0	0,8
	[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	8,0	0,0	0,0	0,0	8,0
ACTIVOS DE HARDWARE	**80 ESTACIONES DE TRABAJO (Portátiles y Escritorio)/HARDWARE**							
	[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.3] Contaminación mecánica	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales.	3	2,7	2,7	0,0	0,0	2,7
	[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0
	[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	6,3	5,0	0,0	0,0	5,0
	[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4 Protección contra las amenazas externas y ambientales.	3	3,3	2,7	0,0	0,0	2,7
	[I.8] Fallo de servicios de comunicacioneS	12.6.1 Gestión de las vulnerabilidades técnicas.	3	5,0	4,0	0,0	0,0	4,0
	[I.9] Interrupción de otros servicios o suministros esenciales	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7	0,0	0,0	2,7
	[I.11] Emanaciones electromagnéticas	11.1.4 Protección contra las amenazas externas y ambientales.	2	4,0	4,0	0,0	0,0	4,0
	[E.24] Caída delsistema por agotamiento de recursos	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0	0,0	0,0	3,0

Tabla 14. (Continuación)

[E.25] Pérdida de equipos	8.1.1 Inventario de activos.	4	1,3	1,3	1,3	0,0	1,3
[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0	0,0	0,0	2,0
[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	4	3,8	3,8	3,0	3,8	2,3
[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
[A.7] Uso no previsto	8.1.3 Uso aceptable de los activos.	2	0,0	0,0	0,0	0,0	4,0
[A.25] Robo de equipos	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0	0,0	1,0
[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	2,5	2,5	0,0	0,0	1,5
[A.27] Ocupación enemiga	11.1.2 Controles físicos de entrada.	4	1,3	1,3	0,0	0,0	1,0
[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	8,0	0,0	0,0	0,0	8,0
2 SERVIDORES (Datos y Reportes)/HARDWARE							
[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.3] Contaminación mecánica	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales.	3	2,7	2,7	0,0	0,0	2,7
[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0

Tabla 14. (Continuación)

	[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	6,3	5,0	0,0	0,0	5,0
	[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4 Protección contra las amenazas externas y ambientales.	3	3,3	2,7	0,0	0,0	2,7
	[I.8] Fallo de servicios de comunicacioneS	12.6.1 Gestión de las vulnerabilidades técnicas.	3	5,0	4,0	0,0	0,0	4,0
	[I.9] Interrupción de otros servicios o suministros esenciales	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7	0,0	0,0	2,7
	[I.11] Emanaciones electromagnéticas	11.1.4 Protección contra las amenazas externas y ambientales.	2	4,0	4,0	0,0	0,0	4,0
	[E.24] Caída delsistema por agotamiento de recursos	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0	0,0	0,0	3,0
	[E.25] Pérdida de equipos	8.1.1 Inventario de activos.	4	1,3	1,3	1,3	0,0	1,3
	[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0	0,0	0,0	2,0
	[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	4	3,8	3,8	3,0	3,8	2,3
	[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
	[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
	[A.7] Uso no previsto	8.1.3 Uso aceptable de los activos.	2	0,0	0,0	0,0	0,0	4,0
	[A.25] Robo de equipos	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0	0,0	1,0
	[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	2,5	2,5	0,0	0,0	1,5
	[A.27] Ocupación enemiga	11.1.2 Controles físicos de entrada.	4	1,3	1,3	0,0	0,0	1,0
	[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	8,0	0,0	0,0	0,0	8,0
ACTIVOS DE RED	**ROUTER LINKSYS/RED**							
	[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3

Tabla 14. (Continuación)

	[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0
	[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	6,3	5,0	0,0	0,0	5,0
	[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4 Protección contra las amenazas externas y ambientales.	3	3,3	2,7	0,0	0,0	2,7
	[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	2,7	2,7	2,7	0,0	2,0
	[E.4] Errores de configuración	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5	0,0	0,0	1,5
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	14.2.2 Procedimientos de control de cambios en los sistemas.	4	2,5	2,0	0,0	0,0	2,0
	[E.25] Pérdida de equipos	8.1.1 Inventario de activos.	4	1,3	1,3	1,3	0,0	1,3
	[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	3,3	3,3	2,7	3,3	2,0
	[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	1,0	1,0	1,0	1,0	0,7
	[A.11] Acceso no autorizado	9.1.1 Política de control de accesos.	4	0,8	0,8	1,3	0,8	0,0
	[A.25] Robo de equipos	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0	0,0	1,0
	[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	0,0	0,0	0,8
	[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	8,0	0,0	0,0	0,0	8,0
	3 SWITCH/RED							
	[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3

Tabla 14. (Continuación)

	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0
	[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	6,3	5,0	0,0	0,0	5,0
	[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4 Protección contra las amenazas externas y ambientales.	3	3,3	2,7	0,0	0,0	2,7
	[E.4] Errores de configuración	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	1,0	0,8	0,0	0,0	0,8
	[E.23] Errores de mantenimiento / actualización de equipos (hardware)	14.2.2 Procedimientos de control de cambios en los sistemas.	4	1,3	1,0	0,0	0,0	1,0
	[E.25] Pérdida de equipos	8.1.1 Inventario de activos.	4	1,3	1,3	1,3	0,0	1,3
	[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	1,7	1,7	1,3	1,7	1,0
	[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	1,0	1,0	1,0	1,0	0,7
	[A.11] Acceso no autorizado	9.1.1 Política de control de accesos.	4	0,8	0,8	1,3	0,8	0,0
	[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	0,0	0,0	0,8
	[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	4,0	0,0	0,0	0,0	4,0
ACTIVOS DE INSTALACIÓN	**CABLEADO ESTRUCTURADO/INSTALACION**							
	[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3

Tabla 14. (Continuación)

[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3	0,0	0,0	1,3
[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	1,3	1,3	1,3	0,0	1,0
[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	0,0	0,0	0,8
[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	4,0	0,0	0,0	0,0	4,0
INSTALACIÓN ELÉCTRICA (Monofásica y Trifásica)/INSTALACION							
[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3	0,0	0,0	1,3
[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0	0,0	3,0

Tabla 14. (Continuación)

	[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	0,0	0,0	0,8
	[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	4,0	0,0	0,0	0,0	4,0
ACTIVOS DE EQUIPAMIENTO AUXILIAR	**1 PLANTA DE ENERGÍA ELÉCTRICA Y 1 UPS 20KVA/EQUIPAMENTO AUXILIAR**							
	[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3	0,0	0,0	1,3
	[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0	0,0	3,0
	[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	0,0	0,0	0,8
	[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	4,0	0,0	0,0	0,0	4,0
ACTIVOS DE SERVICIOS	**SERVICIO DE CONEXIÓN A INTERNET/SERVICIOS**							
	[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3

Tabla 14. (Continuación)

	[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.4] Contaminación electromagnética	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0	0,0	0,0	2,0
	[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	6,3	5,0	0,0	0,0	5,0
	[I.8] Fallo de servicios de comunicaciones	12.6.1 Gestión de las vulnerabilidades técnicas.	3	8,3	6,7	0,0	0,0	6,7
	[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	2,7	2,7	2,7	0,0	2,0
	[E.2] Errores del administrador	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	1,0	1,0	0,0	0,0	0,8
	[E.4] Errores de configuración	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5	0,0	0,0	1,5
	[E.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	1,0	1,0	0,0	0,0	0,0
	[E.24] Caída del sistema por agotamiento de recursos	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0	0,0	0,0	3,0
	[E.25] Pérdida de equipos	8.1.1 Inventario de activos.	4	1,3	1,3	1,3	0,0	1,3
	[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	1,0	1,0	0,0	0,0	1,0
	[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	1,7	1,7	1,3	1,7	1,0
	[A.12] Análisis de tráfico	13.1.1 Controles de red.	4	0,5	0,5	0,0	0,0	0,5
	[A.13] Repudio	9.2.4 Gestión de información confidencial de autenticación de usuarios.	3	1,3	0,0	0,0	0,0	1,0
	[A.14] Interceptación de información (escucha)	9.2.4 Gestión de información confidencial de autenticación de usuarios.	3	0,0	1,3	1,3	1,3	1,3
	[A.16] Introducción de falsa información	9.4.1 Restricción del acceso a la información.	4	1,0	1,0	1,3	1,3	0,8

Tabla 14. (Continuación)

[A.24] Denegación de servicio	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0	0,0	0,0	0,8
[A.25] Robo de equipos	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0	0,0	1,0
[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	0,0	0,0	0,8
SERVICIOS DE MANTENIMIENTO/SERVICIOS							
[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.5] Avería de origen físico o lógico	11.2.4 Mantenimiento de los equipos.	4	5,0	5,0	0,0	0,0	5,0
[I.6] Corte del suministro eléctrico	12.6.1 Gestión de las vulnerabilidades técnicas.	4	6,3	5,0	0,0	0,0	5,0
[I.8] Fallo de servicios de comunicaciones	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7	0,0	0,0	2,7
[E.1] Errores de los usuarios	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	2,7	2,7	2,7	0,0	2,0
[E.2] Errores del administrador	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	2,0	2,0	0,0	0,0	1,5
[E.4] Errores de configuración	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	1,0	0,8	0,0	0,0	0,8
[E.8] Difusión de software dañino	12.2.1 Controles contra el código malicioso.	4	1,0	1,0	0,0	0,0	0,0
[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	1,0	1,0	0,0	0,0	1,0

Tabla 14. (Continuación)

	[A.4] Manipulación de la configuración	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	3,3	3,3	2,7	3,3	2,0
	[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
	[A.17] Corrupción de la información	8.2.2 Etiquetado y manipulado de la información.	3	0,0	1,7	1,7	1,3	1,3
	[A.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0	0,0	1,0
	[A.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	4	0,0	2,0	2,5	0,0	0,0
	[A.24] Denegación de servicio	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0	0,0	0,0	0,8
	[A.25] Robo de equipos	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0	0,0	1,0
	[A.26] Ataque destructivo	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	0,0	0,0	0,8
ACTIVOS DE RECURSO HUMANO	**INGENIERO DE SISTEMAS/PERSONAL**							
	[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3	0,0	0,0	1,3
	[I.8] Fallo de servicios de comunicaciones	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7	0,0	0,0	2,7
	[E.7] Deficiencias en la organización	6.1.1 Asignación de responsabilidades para la segur. de la información.	4	0,0	0,0	0,0	0,0	2,0
	[E.15] Alteración de la información	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3	0,0	1,0
	[E.16] Introducción de falsa información	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3	0,0	1,0
	[E.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	3	1,3	1,7	0,0	0,0	1,7

Tabla 14. (Continuación)

[E.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	3	0,0	2,7	3,3	0,0	2,0
[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0	0,0	0,0	2,0
[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
[A.17] Corrupción de la información	8.2.2 Etiquetado y manipulado de la información.	3	0,0	1,7	1,7	1,3	1,3
[A.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0	0,0	1,0
[A.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	4	0,0	5,0	6,3	0,0	0,0
[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	12,0	0,0	0,0	0,0	12,0
[A.30] Ingeniería social (picaresca)	7.2.2 Concienciación, educación y capacitación en seguridad de la información	4	0,0	6,3	6,3	0,0	5,0
TÉCNICO DE SISTEMAS/PERSONAL							
[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3	0,0	0,0	1,3
[I.8] Fallo de servicios de comunicaciones	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7	0,0	0,0	2,7
[E.7] Deficiencias en la organización	6.1.1 Asignación de responsabilidades para la segur. de la información.	4	0,0	0,0	0,0	0,0	2,0
[E.15] Alteración de la información	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3	0,0	1,0

Tabla 14. (Continuación)

	[E.16] Introducción de falsa información	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3	0,0	1,0
	[E.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	3	1,3	1,7	0,0	0,0	1,7
	[E.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	3	0,0	2,7	3,3	0,0	2,0
	[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0	0,0	0,0	2,0
	[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
	[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
	[A.17] Corrupción de la información	8.2.2 Etiquetado y manipulado de la información.	3	0,0	1,7	1,7	1,3	1,3
	[A.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0	0,0	1,0
	[A.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	4	0,0	5,0	6,3	0,0	0,0
	[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	12,0	0,0	0,0	0,0	12,0
	[A.30] Ingeniería social (picaresca)	7.2.2 Concienciación, educación y capacitación en seguridad de la información	4	0,0	6,3	6,3	0,0	5,0
	150 USUARIOS/PERSONAL							
	[N.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.2] Daños por agua	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[N.*] Desastres naturales	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3	0,0	0,0	1,3
	[I.1] Fuego	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.*] Desastres industriales	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0	0,0	0,0	2,0
	[I.7] Condiciones inadecuadas de temperatura o humedad	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3	0,0	0,0	1,3
	[I.8] Fallo de servicios de comunicaciones	12.6.1 Gestión de las vulnerabilidades técnicas.	3	5,0	4,0	0,0	0,0	4,0

Tabla 14. (Continuación)

[E.7] Deficiencias en la organización	6.1.1 Asignación de responsabilidades para la segur. de la información.	4	0,0	0,0	0,0	0,0	2,0
[E.15] Alteración de la información	9.4.1 Restricción del acceso a la información.	4	2,5	2,5	2,5	0,0	2,0
[E.16] Introducción de falsa información	9.4.1 Restricción del acceso a la información.	4	2,5	2,5	2,5	0,0	2,0
[E.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	3	1,3	1,7	0,0	0,0	1,7
[E.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	3	0,0	3,3	3,3	0,0	2,0
[E.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0	0,0	0,0	2,0
[A.5] Suplantación de la identidad del usuario	9.3.1 Uso de información confidencial para la autenticación.	4	1,5	2,5	2,5	2,5	1,5
[A.6] Abuso de privilegios de acceso	9.2.5 Revisión de los derechos de acceso de los usuarios.	3	2,0	2,0	2,0	2,0	1,3
[A.17] Corrupción de la información	8.2.2 Etiquetado y manipulado de la información.	3	0,0	3,3	3,3	2,7	2,7
[A.18] Destrucción de la información	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0	0,0	1,3
[A.19] Divulgación de información	13.2.4 Acuerdos de confidencialidad y secreto.	4	0,0	5,0	6,3	0,0	0,0
[A.28] Indisponibilidad del personal	7.2.2 Concienciación, educación y capacitación en segur. de la informac.	1	20,0	0,0	0,0	0,0	20,0
[A.30] Ingeniería social (picaresca)	7.2.2 Concienciación, educación y capacitación en seguridad de la información	4	0,0	6,3	6,3	0,0	5,0

Fuente: El autor

7.9 INFORME DE AUDITORÍA

Objetivo de la auditoría: Conocer el estado de la seguridad Informática en la Organización con el fin de dar a conocer los resultados a la Institución para la implementación del plan de mejoramiento por parte de ella.

Fecha de la auditoría: 4 y 5 de octubre del 2016

Fecha de redacción del informe: 30 de noviembre del 2016

Nombre de los auditores: Ingeniero Francisco Javier Hilarión Novoa

Alcance de la auditoría: Unidades funcionales de: contabilidad, presupuesto, activos fijos, compras, tesorería, recursos humanos, contratación, facturación, gerencia de la información, historias clínicas.

Resultados: De acuerdo a las encuestas aplicadas, a la entrevista ejecutada, a la aplicación de verificación de controles ISO 27001:2013 y a las pruebas en campo, mediante Kali Linux, se encuentra lo siguiente:

7.9.1 Copias de seguridad

No se encuentra un procedimiento por escrito. Se encuentra la ejecución de dicho procedimiento, pero con diversas falencias. Las copias de seguridad nunca deben mezclarse con elementos de mantenimiento, ni documentación de otro tipo.

Las copias de seguridad deben almacenarse en lo posible en un lugar diferente a la oficina de gerencia de la información y bajo una infraestructura que asegure su estado físico y lógico.

No fue permitida una prueba de recuperación que garantice la confiabilidad del procedimiento actual. Es importante que se rediseñe el procedimiento, donde se contemple la prueba de recuperación con una frecuencia de una vez cada mes.

7.9.2 Infraestrutura de redes

El rack principal de comunicaciones, debe estar aislado de la oficina de Gerencia de la información. No deben almacenarse monitores en el rack de comunicaciones.

Deben etiquetarse los patch cord de las redes, con el fin de encontrar daños rápidamente.

Debe adecuarse el rack, organizar los cables, realizar el procedimiento de marquillado de los cables instalación de un switch KVM y documentar el cableado adecuadamente.

7.9.3 Acceso físico

No se tiene implementado un mecanismo de acceso físico, donde se registre información de las personas o usuarios que ingresan o salen de la institución, por ejemplo, un sistema de biometría.

La tarea de monitorización a través del circuito cerrado de televisión, debe ser responsabilidad del personal de seguridad quien contará con una terminal de monitoreo en diferentes puntos.

7.9.4 Redes inalámbricas

Se evidencia que la red wifi de la institución, cuenta con SSID oculto, lo cual esta dentro de las buenas practicas, además cuenta con tecnología WPA2 PSK. Más sin embargo se recomienda que esta red no tenga alcance fuera de los predios de la Institución, ya que se filtra la señal y puede ser objeto de sniffeo y capturas. También se evidencia que no se cambia la contraseña de acceso periódicamente, lo cual debe realizarse al menos una vez por mes.

Ya que la red WiFi de la institución, esta destinada a la conexión de computadores portátiles de auxiliares de talento humano, contabilidad y otros, debe restringirse el uso a dispositivos móviles, ya que por medio de la auditoría a la captura de paquetes con el software Wireshark, se evidenciaron descargas desde la Play Store y en los procesos del Hospital no se evidencia el uso de dispositivos móviles.

7.9.5 Firewall

Las políticas de firewall, no se encuentran definidas y en algunos equipos el cortafuegos esta descativado, lo cual indica graves peligros para la seguridad de la información.

Se encuentra que los equipos tienen fácil acceso a cuentas de facebok, youtube, radio online, lo cual afecta la disponibilidad de la información y se presta para distracción de los funcionarios. Además, es un vector de fácil infección por Ingeniería Social.

Se deben establecer políticas restrictivas en este aspecto.

Por otra parte, analizando los puertos de los equipos y del servidor, se encuentra que todos están en estado abierto, lo cual es grave, teniendo en cuenta que se ejecutan servicios de apache, mysql y php.

De continuar con los puertos abiertos, sin políticas restrictivas en el firewall, podrán realizarse ataques de fácil explotación en el medio y afectar la disponibilidad, integridad y confidencialidad de la información. Por ello se recomienda la instalación de un UTM con firewall, control de tráfico, seguridad perimetral y generación de resportes de seguridad.

7.9.6 Antivirus

La Institución, no cuenta con un antivirus instalado en todos sus equipos, lo cual indica graves vulnerabilidades contra código malicioso que pueda llegar a filtrarse.

No cuentan con una solución corporativa administrada que permita hacer un seguimiento a los incidentes, asi como la administración de toda la suite.

7.9.7 Contraseñas

Es de vital importancia instalar un servicio de directorio donde se puedan centralizar los usuarios, con políticas de seguridad, restricciones y niveles de administración, por ejemplo, la instalación de active directory.

7.9.8 Ingeniería social

El personal de la institución, desconoce del tema Seguridad Informática e Ingeniería Social y no tiene nociones de protección ante este tipo de ataques. Se recomienda ampliamente hacer jornadas de sensibilización y capacitación en Seguridad Informática.

7.9.9 Gestión de la seguridad de la información

La oficina de Gerencia de la Información, no cuenta con un manual de seguridad de la información ni de contingencias.

No cuenta con los procesos, procedimientos ni protocolos documentados de sus actividades ni de la Seguridad de la Información, de acuerdo a la norma ISO 27001:2013.

7.9.10 Organización y aspecto

La oficina de Gerencia de la Información, se encuentra desordenada, se mezclan equipos en buen estado y equipos en mal estado, repuestos, tintas, copias de seguridad y el aspecto de los escritorios muestra gran desorganización, lo que posibilita la pérdida de información relevante y la no optimización de tiempo y recursos.

Conclusiones:

- No cuenta con la documentación del área de gerencia de la información
- No cuenta con los procesos y procedimientos documentados
- La mayoría de puertos se encuentran abiertos
- No hay un proceso establecido de copias de seguridad
- No cuenta con procedimientos de asignación de contraseñas
- La oficina se encuentra en mal aspecto
- No hay un plan de capacitaciones en Seguridad informática para el personal de la organización
- No hay un plan de contingencia para garantizar la continuidad del negocio.

Recomendaciones técnicas:

- Se debe diseñar, implementar, socializar y hacer seguimiento a un procedimiento de backup
- Se debe establecer un espacio adecuado para seguimiento del sistema de cámaras de videovigilancia
- Debe implementarse un sistema de control de acceso biométrico
- Limitar el alcance de la red WIFI
- Establecer un procedimiento de asignación y cambio de claves periódicas al WIFI
- Bloquear acceso a Facebook, YouTube y Radio Online. Activarlas solo a determinadas horas del día, ejemplo la hora del almuerzo.

- Monitorear el estado de los puertos abiertos para evitar ataques por este medio.
- Crear un procedimiento de asignación de contraseñas a los equipos y realizar el respectivo seguimiento al mismo.
- Instalar un antivirus, actualizarlo y licenciarlo.
- Crear un plan de capacitación en seguridad informática para el personal de la Institución
- Crear la documentación del área, principalmente el Sistema de Gestión de la Seguridad de la Información, los procesos, procedimientos y protocolos.
- Elaborar una jornada de limpieza y organización de la Oficina de Gerencia de la Información.
- Realizar estricto seguimiento al plan de mantenimiento
- Implementar los siguientes controles de la norma ISO 27001:2013.

    - 11.1.4 Protección contra las amenazas externas y ambientales.
    - 11.2.4 Mantenimiento de los equipos.
    - 12.6.1 Gestión de las vulnerabilidades técnicas.
    - 7.2.2 Concienciación, educación y capacitación en seguridad de la información.
    - 12.2.1 Controles contra el código malicioso.
    - 9.4.1 Restricción del acceso a la información.
    - 12.3.1 Copias de seguridad de la información.
    - 13.2.4 Acuerdos de confidencialidad y secreto.
    - 9.3.1 Uso de información confidencial para la autenticación.
    - 9.2.5 Revisión de los derechos de acceso de los usuarios.
    - 9.1.1 Política de control de accesos.
    - 16.1.2 Notificación de los eventos de seguridad de la información.
    - 12.6.1 Gestión de las vulnerabilidades técnicas.
    - 11.2.4 Mantenimiento de los equipos.

8. CRONOGRAMA DE ACTIVIDADES

El cronograma de actividades se establece mediante el siguiente diagrama de Gantt.

Tabla 14. Diagrama de Gantt

ACTIVIDADES	SEPTIEMBRE				OCTUBRE				NOVIEMBRE			
	1	2	3	4	1	2	3	4	1	2	3	4
Planeación de la auditoría: elaboración del plan auditor que contiene la definición de objetivos, alcance, equipo, instrumentos y técnicas a emplear			15 de septiembre									
Realización de encuestas al personal de la Institución seleccionado, acerca del tema seguridad informática					4 de octubre							
Realización de entrevistas a los encargados de la unidad funcional de gerencia de la Información					4 de octubre							
Ejecución de la auditoría: aplicación de técnicas, procedimientos e instrumentos					5 de octubre							

Tabla 14. (Continuación)

Elaboración de dictamen: identificación de oportunidades de mejoramiento												30 de Noviembre

Fuente: El autor

9. IMPACTO Y RESULTADOS

La Gerencia de la organización y la Gerencia de la información, encuentran en el proyecto un gran apoyo para abordar las problemáticas evidenciadas en la auditoría. La organización no era consiente de la gran cantidad de vulnerabilidades e inconvenientes que presentaba su departamento de sistemas y por medio de este proyecto se consientizaron y empezaron su proceso de elaboración de plan de mejoramiento, sensibilización y capacitación para subsanar las problemáticas evidenciadas.

La organización empezará su proceso de diseño, implementación y seguimiento del plan de auditorías al departamento de Sistemas, con el fin de minimizar los riesgos por pérdida de confidencialidad en los registros financieros y de historia clínica de la Institución.

La Institución implementará dentro del plan de mejoramiento un estricto seguimiento a los controles recomendados en el informe de auditoría.

10. DIVULGACIÓN Y RECOMENDACIONES

10.1 DIVULGACIÓN

- Comunicación directa al líder de Gerencia de la Información
- Comunicación directa al Gerente del Hospital
- Reunión informativa con los líderes de las Unidades funcionales involucradas
- Sustentación ante el jurado designado por la Universidad Nacional Abierta y a Distancia UNAD
- Publicación en el repositorio Institucional de la Universidad Nacional Abierta y a Distancia UNAD

10.2 RECOMENDACIONES

Según la auditoría se encuentran diversas amenazas a las que está expuesta la información del Hospital San Francisco de Gachetá, por dicho motivo se hace necesario implementar un plan de mejoramiento para el informe de auditoría que se ha descrito en el proyecto y elaborar un seguimiento trimestral al mismo.

Se debe guardar las copias de seguridad de la información en un lugar diferente a la oficina de gerencia de la información.

Es necesario que el Hospital San Francisco de Gachetá gestione con los funcionarios del área de gerencia de la información, capacitación en seguridad informática y de esa forma sensibilizar y capacitar al personal en general.

Según la auditoría se encuentran diversas amenazas a las que está expuesta la información del Hospital San Francisco de Gachetá, se hace necesario implementar un plan de mejoramiento para el informe de auditoría que se ha descrito en el proyecto y elaborar un seguimiento trimestral al mismo.

Se debe guardar las copias de seguridad de la información en un lugar diferente a la oficina de gerencia de la información.

Es importante instalar un UTM con firewall, control de tráfico, seguridad perimetral y generación de reportes de seguridad.

Es importante instalar un servicio de directorio activo con el fin de centralizar los usuarios y establecer políticas de seguridad.

Es vital contratar una solución de protección antivirus, con el fin de realizar seguimiento a los incidentes generados,

Se requiere instalar un control de acceso para administar el ingreso y egreso del personal a la institución.

Debe de trasladarse la monitorización de el circuito cerrado de televisión al personal de seguridad de la Institución.

Rediseñar el rack de comunicaciones y organizar el cableado correcta y ordenadamente,

Establecer un área específica para insumos de mantenimiento y no mezclarlo con la parte documental ni con los registros de backups.

Organizar el área de Gerencia de la Información en general.

Documentar todos los procedimientos y protocolos del área de Gerencia de la Información.

Es necesario que el Hospital San Francisco de Gachetá gestione con los funcionarios del área de gerencia de la información, conocimientos avanzados en seguridad informática y de esa forma sensibilizar y capacitar al personal en general.

11. CONCLUSIONES

- La auditoría de seguridad informática en el Hospital San Francisco de Gachetá ha permitido evidenciar las diferentes vulnerabilidades y amenazas a las que se ven expuestas los activos de información del área administrativa y de historias clínicas del hospital San Francisco de Gachetá por lo que es importante que se tomen medidas para proteger los activos de información y garantizar la continuidad del negocio.

La Organización actualmente, no cuenta con la documentación del área de gerencia de la información, no cuenta con los procesos y procedimientos documentados, según la auditoria realizada, la mayoría de puertos escucha en los terminales se encuentran abiertos, no hay un procedimiento ni politica establecida de copias de seguridad, no cuenta con procedimientos de asignación de contraseñas, la oficina se encuentra en mal aspecto, no hay un plan de capacitaciones en Seguridad informática para el personal de la organización, no hay un plan de contingencia para garantizar la continuidad del negocio, no hay un estricto seguimiento al plan de mantenimiento, no hay un antivirus de protección y no cuentas con un firewall ni políticas de configuración del firewall individual de los terminales.

- Utilizando la Metodología MAGERIT V3 se ha realizado la identificación de cada una de las amenazas por activo informático y junto con ella la evaluación del riesgo analizando los impactos en cada uno de los activos y se han establecido controles los cuales deben aplicarse según el análisis para proteger los activos informáticos en cada una de las dimensiones en las que se ven afectados.

- El informe de auditoría permitirá al Hospital generar su plan de mejoramiento y su posterior seguimiento, con el fin de garantizar la minimización de la pérdida de confidencialidad de la información contenida en los registros financieros y de historias clínicas.

El plan de mejoramiento debe realizarse como primera medida en base a las recomendaciones entregadas en el ítem de recomendaciones del informe de auditoría y sus controles asociados de acuerdo a la norma ISO 27001:2013

Se deben implementar acciones de mejoramiento primordialmente en cuanto a la cantidad de puertos abiertos en cada uno de los equipos escaneados mediante NMAP. También generar un plan de capacitaciones en seguridad informática y documentar los procesos, procedimientos, protocolos y manuales del área de Gerencia de la información, con el fin de proceder a evaluar el cumplimiento de los mismos mediante los planes de acción asociados a cada documento.

BIBLIOGRAFIA

SEGURIDAD INFORMÁTICA SMR. Seguridad Informática. [consultado 17 marzo de 2016]. Disponible en internet: https://seguridadinformaticasmr.wikispaces.com/TEMA+1+SEGURIDAD+IFORM%C3%81TICA

COSTAS SANTOS, Jesús. Seguridad y alta disponibilidad. 1 ed. Ediciones RA-MA, 2014. p. 10.

ECURED. Seguridad informática. [consultado 20 marzo de 2016]. Disponible en: http://www.ecured.cu/Seguridad_Inform%C3%A1tica

CEEISEC. Sistema de gestión de la seguridad de la información. [consultado 25 marzo de 2016]. Disponible en: www.ceeisec.com/nuevaweb/doc/FORMACION_SGSI_2010.pdf

RED Y SEGURIDAD. Política de seguridad informática. [consultado 25 de marzo de 2016]. Disponible en: www.redyseguridad.fi-p.unam.mx/proyectos/tsi/capi/Cap4.html

ADVISERA. Norma ISO 27001. [consultado 25 de marzo de 2016]. Disponible en: http://advisera.com/27001academy/es/que-es-iso-27001/

ADMINISTRACIÓN ELECTRÓNICA. Metodología de Análisis y Gestión de riesgos de los sistemas de información. [consultado 25 de marzo de 2016]. Disponible en: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html

CENTRO DE TRANSFERENCIA TECNOLÓGICA. Libro I método. [consultado 25 de marzo de 2016]. Disponible en: http://administracionelectronica.gob.es/ctt/resources/Soluciones/184/Area%20descargas/Libro-I-Metodo.pdf?idIniciativa=184&idElemento=85

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Auditoría Informática. [consultado 25 de marzo de 2016]. Disponible en: http://datateca.unad.edu.co/contenidos/233004/riesgos/leccin_27_fases_de_la_auditora_informtica_y_de_sistemas.html

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Módulo Auditoría de Sistemas. [consultado 25 de marzo de 2016]. Disponible en: http://datateca.unad.edu.co/contenidos/90168/2014MODULO_90168_plantilla_unidad_2.pdf

TÚ GUÍA CONTABLE. Normas de auditoria generalmente aceptadas. [consultado 25 de marzo de 2016]. Disponible en: www.tuguiacontable.org/app/article.aspx?id=119

UNICAUCA. Elaboración de programas de auditoría. [consultado 25 de marzo de 2016]. Disponible en: www.fccea.unicauca.edu.co/old/tgarf/tgarfse67.html

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Ciclo PDCA. [consultado 25 de marzo de 2016]. Disponible en: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html

TECNOLOGÍAS AVG. Accesibilidad. [consultado 25 de marzo de 2016]. Disponible en: http://www.tecnologiasavg.com/index.php/component/k2/item/105-sistema-de-gestion-de-seguridad-de-la-informacion

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Autenticidad. [consultado 25 de marzo de 2016]. Disponible en: http://datateca.unad.edu.co/contenidos/233011/233011Exe/leccin_11_autenticidad.html

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Integridad. [consultado 25 de marzo de 2016]. Disponible en: http://datateca.unad.edu.co/contenidos/233011/233011Exe/leccin_13_integridad.html

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Confidencialidad. [consultado 25 de marzo de 2016]. Disponible en: http://datateca.unad.edu.co/contenidos/233011/233011Exe/leccin_12_confidencialidad.html

ANEXOS

ANEXO A. ENCUESTA: CONOCIMIENTOS BÁSICOS EN SEGURIDAD INFORMÁTICA

Personas a aplicar: 12, las cuales son los líderes de los siguientes procesos (cartera, contabilidad, presupuesto, activos fijos, compras, tesorería, recursos humanos, contratación, facturación, gerencia de la información, historias clínicas y un equipo de consulta externa).

Objetivo: Determinar el grado de conocimientos en el área de seguridad informática, de los líderes de procesos del Hospital San Francisco de Gachetá, con el fin de establecer un plan de mejoramiento.

Enunciado: Estimado funcionario de la E.S.E Hospital San Francisco de Gachetá, tenga la amabilidad de responder con total sinceridad las siguientes preguntas, con el fin de establecer un plan de mejoramiento que vele por la seguridad, integridad y confidencialidad de la información manejada en su área.

1. ¿Tiene instalado un antivirus?

- Si
- No
- No sé para qué sirve

2. ¿En qué estado se encuentra el firewall de su computador?

- Activado
- Desactivado
- No sé qué es un firewall

3. ¿Con que frecuencia analiza su computador con un antivirus?

- Semanalmente

- Mensualmente
- No lo analizo

4. ¿Tiene instalado un software Antispyware?
- Si
- No
- No sé para qué sirve

5. Si en este momento se daña su equipo de cómputo, ¿Tiene usted una copia de seguridad de su información?
- Si
- No
- No sé para qué sirve una copia de seguridad

6. ¿Dónde tiene anotada la clave de acceso a su equipo de cómputo?
- En la agenda
- En un papel que guardo en el escritorio
- En el teléfono móvil
- En un lugar bajo llave
- No la tengo anotada

7. Su clave de acceso al computador tiene alguna similitud con:
- Fecha de nacimiento de un familiar
- Fecha importante
- Nombre de un familiar
- Nombre de un lugar importante
- Número de un documento
- Ninguna de las anteriores

8. La contraseña de acceso al computador tiene:

- Números
- Letras
- Números y letras
- Números, letras y símbolos especiales
- No tengo contraseña

ANEXO B. ENTREVISTA AL LÍDER DE SEGURIDAD DE LA INFORMACIÓN

La entrevista contempla los siguientes puntos.

1- Se solicita al líder de Gerencia de la información que explique cada uno de los procedimientos solicitados en el ítem de documentación requerida

Tabla 15. Documentación requerida

DOCUMENTACIÓN REQUERIDA	SOCIALIZACIÓN
Sistema de Gestión de Seguridad Informática	No existe este documento
Certificación de estudios del Líder de Gerencia de la Información	El líder de Seguridad de la información certifica sus estudios como Ingeniero de Sistemas
Inventario de activos informáticos	El inventario de activos concuerda con la base de datos de activos fijos de la institución
Matriz de riesgos de Seguridad Informática	Se miden 5 riesgos, los cuales están inmersos en el mapa de riesgos del área de control interno.
Planes de mejoramiento de Seguridad Informática	No existen.
Plan de contingencia Seguridad de la Información	El plan de contingencia es básico para la complejidad que requiere la institución y se enfoca en el uso de la planta eléctrica de respaldo y el uso de una UPS para los servicios de red de la Institución.

Tabla 16. (Continuación)

Procedimiento de asignación de credenciales a los usuarios	No existe, se realiza empíricamente.
Procedimiento de asignación de contraseñas a la red WIFI	No existe, se realiza empíricamente.
Procedimiento de ingreso del personal a la Institución	Los funcionarios ingresan a la institución por medio de control de acceso biométrico y semanalmente se evalúan estos registros.
Procedimiento de egreso del personal a la Institución	Los funcionarios egresan a la institución por medio de control de acceso biométrico y semanalmente se evalúan estos registros.
Procedimiento de generación de contraseñas	No existe, se realiza empíricamente.
Procedimiento de ejecución de Backups	No existe, se realiza empíricamente.
Procedimiento de Manejo de discos extraíbles	No existe, se realiza empíricamente.
Procedimiento de control de acceso a internet	No existe, se realiza empíricamente.

Tabla 16. (Continuación)

Cronograma de mantenimiento de activos informáticos	Existe y está ligado al plan de mantenimiento hospitalario, liderado por el departamento de Ingeniería Biomédica. El cronograma indica que se realiza un mantenimiento preventivo cada seis meses por cada activo informático.
Reportes de mantenimiento de activos informáticos	Existen los reportes, estos se adjuntan a las hojas de vida de cada equipo. Allí se consignan los datos del equipo, fecha, responsable y actividad ejecutada.
Hojas de vida de activos informáticos	Las hojas de vida de los activos infromáticos, están almacenados en el repositorio en archivo físico y tienen adjunto la documentación legal de cada equipo y sus respectivos historiales de mantenimiento.
Compromiso de confidencialidad firmado por funcionarios	No existe.
Actas de capacitación a los usuarios internos en Seguridad Informática	No existen.
Fotografías de capacitación a los usuarios internos en Seguridad Informática	No existe.

Fuente: El autor

2- Se solicita al líder de Gerencia de la información que explique el Sistema de Gestión de Seguridad Informática

El líder de gerencia de la información afirma que no se tiene implementado un sistema de Gestión de seguridad informática, ya que el tiempo asignado para sus actividades es muy limitado.

3- Se solicita al líder de Gerencia de la información que explique la matriz de riesgos

El líder de gerencia de la información, indica que los riesgos para el área de sistemas, se encuentran consignados en el mapa de riesgos institucional, a cargo del área de control interno.

Se miden los siguientes riesgos:

- ✓ Falta de capacitación al personal en el área de herramientas informáticas.
- ✓ Falta de capacitación al personal en el uso del equipo informático.
- ✓ Falta de un plan de mantenimiento de activos informáticos.
- ✓ Incumplimiento en el cronograma de mantenimiento de activos informáticos.
- ✓ Incumplimiento en el cronograma de backups.

4- Se solicita al líder de Gerencia de la información que socialice los planes de mejoramiento de seguridad informática y evidencie los seguimientos a los mismos.

El líder de gerencia de la información asegura que la falta de tiempo y la falta de recurso humano le limitan para el diseño de planes de mejoramiento para la seguridad informática.

5- Se solicita al líder de Gerencia de la información que dé a conocer el inventario de activos informáticos y su respectiva ubicación de cada activo.

El líder de gerencia de la información muestra un archivo en Excel, el cual concuerda con la base de datos de activos fijos de la Institución, verificando así el inventario.

6- Se solicita al líder de Gerencia de la información que socialice el plan de mantenimiento, cronograma y reportes.

El líder de gerencia de la información muestra un plan de mantenimiento que envían a la secretaria de salud, el cual indica claramente las actividades llevadas a cabo en el área.

Dicho plan de mantenimiento, especifica uno a uno los seriales, marcas, número de inventario, encargado de mantenimiento, fecha de mantenimiento y el procedimiento de mantenimiento para cada equipo.

Se verifica que el cronograma de mantenimiento se cumple parcialmente.

El líder de gerencia de la información muestra los reportes de mantenimiento, lo cual evidencia que se están realizando.

7- Se solicita al líder de Gerencia de la información que dé a conocer el archivo documental de hojas de vida de los activos informáticos

El líder de gerencia de la información indica que existe un repositorio en archivo físico, donde se almacenan las hojas de vida de los activos informáticos, lo cual se evidencio por medio de la observación, ya que está prohibida la toma de fotografías en dichas áreas de la institución.

El repositorio de hojas de vida no se encuentra digitalizado ni gestionado por ningún tipo de software.

ANEXO C LISTA DE CHEQUEO ISO 27001:2013

ISO 27001:2013 (ANEXO A) E.S.E. HOSPITAL SAN FRANCISCO DE GACHETA			
OBJETIVOS DE CONTROL Y CONTROLES			**CUMPLE (SI/NO)**
A.5. POLÍTICA DE LA SEGURIDAD DE LA INFORMACIÓN.	A.5.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información.	A.5.1.1. Políticas para la Seguridad de la Información. Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la Dirección, publicada y comunicada a los empleados y partes interesadas.	**NO**
	Objetivo. Brindar orientación y soporte, por parte de la dirección, de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.	A.5.1.2. Revisión de las Políticas para seguridad de la información. Las Políticas para Seguridad de la Información se deben revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su idoneidad, adecuación y eficacia continúas.	**NO**
A.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	A.6.1. Organización Interna.	A.6.1.1. Seguridad de la Información Roles y Responsabilidades. Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	**NO**
	Objetivo. Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación del SGSI.	A.6.1.2. Separación de deberes. Las tareas y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la organización.	**NO**
		A.6.1.3. Contacto con las autoridades. Se debe mantener contactos apropiados con las autoridades pertinentes.	**NO**
		A.6.1.4. Contacto con grupos de interés especial. Se deben mantener controles apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.	**NO**
		A.6.1.5. Seguridad de la información en Gestión de Proyectos. La seguridad de la información se debe tratar en la gestión de proyectos, independiente del tipo de proyecto,	**NO**
	A.6.2. Dispositivos Móviles y Teletrabajo.	A.6.2.1. Política para dispositivos móviles. Se deben adoptar una política y unas medidas de	**NO**

		seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	
	Objetivo. Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.	A.6.2.2. Teletrabajo. Se deben implementar una política y medidas de seguridad de soporte para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	**NO**
A.7. SEGURIDAD DE LOS RECURSOS HUMANOS.	A.7.1. Antes de asumir el empleo.	A.7.1.1. Selección. Las verificaciones de los antecedentes de todos los candidatos a un empleo se deben llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deben ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.	**SI**
	Objetivo. Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.	A.7.1.2. Términos y condiciones del empleo. Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a seguridad de la información.	**NO**
	A.7.2. Durante la ejecución del empleo.	A.7.2.1. Responsabilidades de la Dirección. La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos de la organización.	**NO**
	Objetivo. Asegurarse que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.	A.7.2.2. Toma de conciencia, educación y formación de la Seguridad de la Información. Todos los empleados de la organización y donde sea pertinente, los contratistas deben recibir educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.	**NO**
		A.7.2.3. Proceso disciplinario. Se debe contar con un proceso formal y comunicado para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.	**NO**
	A.7.3. Terminación y cambio de empleo.	A.7.3.1. Terminación o cambio de responsabilidades de empleo. Las responsabilidades y los deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir, comunicar al empleado o contratista y se deben hacer cumplir.	**SI**

	Objetivo. Proteger los intereses de la organización como parte del proceso de cambio o terminación del empleo.		
A.8. GESTIÓN DE ACTIVOS.	A.8.1. Responsabilidad por los Activos.	A.8.1.1. Inventario de Activos. Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	**NO**
	Objetivo. Identificar los activos organizacionales y definir las responsabilidades de protección apropiada.	A.8.1.2. Propiedad de los activos. Los activos mantenidos en el inventario deben ser propios.	**NO**
		A.8.1.3. Uso Aceptable de los Activos. Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	**NO**
		A.8.1.4. Devolución de Activos. Todos los empleados y usuarios de partes externas deben devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.	**NO**
	A.8.2. Clasificación de la Información.	A.8.2.1. Clasificación de la Información. La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.	**NO**
	Objetivo. Asegurar que la organización recibe un nivel apropiado de protección de acuerdo con su importancia para la organización.	A.8.2.2. Etiquetado de la Información. Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.	**NO**
		A.8.2.3. Manejo de Activos. Se deben desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.	**NO**
	A.8.3. Manejo de medios de soporte.	A.8.3.1. Gestión de medios de Soporte Removibles. Se deben implementar	**NO**

		procedimientos para la gestión de medios de soporte removibles, de acuerdo con el esquema de clasificación adoptado por la organización.	
	Objetivo. Prevenir la divulgación, la modificación, el retiro o la destrucción de información almacenada en medios de soporte.	A.8.3.2. Disposición de los medios de soporte. Se debe disponer en forma segura de los medios de soporte cuando ya no se requieran, utilizando procedimientos formales.	**NO**
		A.8.3.3. Transferencia de medios de soporte físicos. Los medios que contienen información se deben proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.	**NO**
A.9. CONTROL DE ACCESO.	A.9.1. Requisitos del Negocio para Control de Acceso.	A.9.1.1. Política de Control de Acceso. Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.	**SI**
	Objetivo. Limitar el acceso a información y a instalaciones de procesamiento de información.	A.9.1.2. Acceso a redes y a servicios en red. Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	**SI**
	A.9.2. Gestión de Acceso de Usuarios.	A.9.2.1. Registro y cancelación del registro de usuarios. Se debe implementar un proceso formal de registro y de cancelación del registro para posibilitar la asignación de los derechos de acceso.	**NO**
	Objetivo. Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.	A.9.2.2. Suministro de acceso de usuarios. Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o cancelar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.	**SI**
		A.9.2.3. Gestión de derechos de acceso privilegiado. Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado.	**SI**
		A.9.2.4. Gestión de información de autenticación secreta de usuarios. La asignación de información de autenticación secreta se debe controlar por medio de un procedimiento de gestión formal.	**SI**
		A.9.2.5. Revisión de los derechos de acceso de usuarios. Los dueños de los activos deben revisar los derechos de acceso de los usuarios a intervalos regulares.	**NO**

		A.9.2.6. Cancelación o ajuste de los derechos de acceso. Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procedimiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios.	**SI**
	A.9.3. Responsabilidades de los usuarios.	A.9.3.1.Uso de información secreta. Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.	**NO**
	Objetivo. Hacer que los usuarios rindan cuentas por la custodia de su información de autenticación.		
	A.9.4. Control de Acceso a Sistemas y Aplicaciones.	A.9.4.1. Restricción de acceso a información. El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	**SI**
	Objetivo. Prevenir el uso no autorizado de sistemas y aplicaciones.	A.9.4.2. Procedimiento de Conexión Segura. Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de conexión segura.	**SI**
		A.9.4.3. Sistema de Gestión de Contraseñas.los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.	**NO**
		A.9.4.4. Uso de programas utilitarios privilegiados. Se debe restringir y controlar estrechamente el uso de programas utilitarios que podrían tener capacidad de anular el sistema y los controles de las aplicaciones.	**NO**
		A.9.4.5. Control de Acceso a Códigos Fuente de Programas. Se debe restringir el acceso a códigos fuente de programas.	**NO**
A.10. CRIPTOGRAFÍA	A.10.1. Controles Criptográficos.	A.10.1.1. Política sobre el uso de controles Criptográficos. Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para protección de información.	**NO**

	Objetivo. Asegurar el uso apropiado y eficaz de la criptografía para proteger la confiabilidad, la autenticidad y/o la integridad de la información.	A.10.1.2. Gestión de Claves. Se debe desarrollar e implementar una política sobre el uso, protección y tiempo de vida de claves criptográficas, durante todo su ciclo de vida.	**NO**
A.11. SEGURIDAD FÍSICA Y AMBIENTAL.	A.11.1. Áreas Seguras.	A.11.1.1. Perímetro de Seguridad Física. Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.	**SI**
	Objetivo. Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.	A.11.1.2. Controles Físicos de entrada. Las áreas seguras se deben proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.	**SI**
		A.11.1.3. Seguridad de oficinas, salones e instalaciones. Se debe diseñar y aplicar seguridad física a oficinas, salones e instalaciones.	**SI**
		A.11.1.4. Protección contra amenazas externas y ambientales. Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	**SI**
		A.11.1.5. Trabajo en áreas seguras. Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.	**SI**

		A.11.1.6. Áreas de despacho y carga. Se deben controlar los puntos de acceso tales como áreas de despacho y de carga y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.	**SI**
	A.11.2. Equipos.	A.11.2.1. Ubicación y protección de los equipos. Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros ambientales y las posibilidades de acceso no autorizado.	**SI**
	Objetivo. Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.	A.11.2.2. Servicios Públicos de soporte. Los equipos se deben proteger de fallas de potencia y otras interrupciones causadas por fallas en los servicios públicos de soporte.	**SI**
		A.11.2.3. Seguridad del cableado. El cableado de potencia y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptaciones, interferencia o daño.	**SI**
		A.11.2.4. Mantenimiento de equipos. Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	**SI**
		A.11.2.5. Retiro de Activos. Los equipos, información o software no se deben retirar de su sitio sin autorización previa.	**SI**
		A.11.2.6. Seguridad de equipos y activos fuera del predio. Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de los predios de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichos predios.	**SI**
		A.11.2.7. Disposición segura o reutilización de equipos. Se deben verificar todos los elementos de equipos que contengan medios de almacenamiento para asegurar que cualquier dato confidencial o software con licencia haya sido retirado o sobre escrito en forma segura antes de su disposición o reuso.	**SI**
		A.11.2.8. Equipos sin supervisión de los usuarios. Los usuarios deben asegurarse de que el equipo sin supervisión tenga la protección apropiada.	**SI**

		A.11.2.9. Política de escritorio limpio y pantalla limpia. Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.	**SI**
A.12. SEGURIDAD DE LAS OPERACIONES.	A.12.1. Procedimientos operacionales y responsabilidades.	A.12.1.1. Procedimientos de operación documentadas. Los procedimientos operativos se deben documentar y poner a disposición de todos los usuarios que los necesitan.	**NO**
	Objetivo. Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.	A.12.1.2. Gestión de Cambios. Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	**NO**
		A.12.1.3. Gestión de Capacidad. Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	**NO**
		A.12.1.4. Separación de los ambientes de desarrollo, ensayo y operación. Se deben separar los ambientes de desarrollo, ensayo y operativos, para reducir los riesgos de acceso o cambios no autorizados al ambiente operacional.	**NO**
	A.12.2. Protección contra códigos maliciosos.	A.12.2.1. Controles contra códigos maliciosos. Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	**NO**
	Objetivo. Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.		
	A.12.3. Copias de Respaldo.	A.12.3.1. Copias de respaldo de la información. Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	**NO**
	Objetivo. Proteger contra la pérdida de datos.		
	A.12.4. Registro y Seguimiento.	A.12.4.1. Registro de eventos. Se deben elaborar, conservar y revisar regularmente los registros de eventos acerca de actividades del usuario,	**NO**

		excepcionales, fallas y eventos de seguridad de la información.	
	Objetivo. Registrar eventos y generar evidencia.	A.12.4.2. Protección de la información de registro. Las instalaciones y la información de registro se deben proteger contra alteración y acceso no autorizado.	**NO**
		A.12.4.3. Registros del administrador y del operador. Las actividades del administrador y del operador del sistema se deben registrar y los registros se deben proteger y revisar con regularidad.	**NO**
		A.12.4.4. Sincronización de relojes. Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deben sincronizar con una única fuente de referencia de tiempo.	**SI**
	A.12.5. Control de Software Operacional.	A.12.5.1. Instalación de software en sistemas operativos. Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	**NO**
	Objetivo. Asegurarse de la integridad de los sistemas operacionales.		
	A.12.6. Gestión de vulnerabilidad técnica.	A.12.6.1. Gestión de las vulnerabilidades técnicas. Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	**NO**
	Objetivo. Prevenir el aprovechamiento de las vulnerabilidades técnicas.	A.12.6.2. Restricciones sobre la instalación de Software. Se debe establecer e implementar el reglamento de instalación de software por parte de los usuarios.	**NO**
	A.12.7. Consideraciones sobre auditorías de sistemas de información.	A.12.7.1. Controles sobre auditorías de Sistemas de Información. Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	**NO**
	Objetivo. Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.		

A.13. SEGURIDAD DE LAS COMUNICACIONES.	A.13.1. Gestión de Seguridad de Redes.	A.13.1.1. Controles de redes. Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	**NO**
	Objetivo. Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.	A.13.1.2. Seguridad de los servicios de red. Se deben identificar los mecanismos de seguridad y los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	**NO**
		A.13.1.3. Separación en las redes. Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	**NO**
	A.13.2. Transferencia de información.	A.13.2.1. Políticas y procedimientos de transferencia de información. Se debe contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información, mediante el uso de todo tipo de instalaciones de comunicaciones.	**NO**
	Objetivo. Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.	A.13.2.2. Acuerdos sobre transferencia de información. Los acuerdos deben tratar la transferencia segura de información del negocio entre la organización y las partes externas.	**NO**
		A.13.2.3. Mensajes electrónicos. Se debe proteger apropiadamente la información incluida en los mensajes electrónicos.	**NO**
		A.13.2.4. Acuerdos de confidencialidad o de no divulgación. Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.	**NO**
A.14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.	A.14.1. Requisitos de seguridad de los sistemas de información.	A.14.1.1. Análisis y especificación de requisitos de seguridad de la información. Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	**NO**

	Objetivo. Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye los requisitos para sistemas de información que prestan servicios sobre redes públicas.	A.14.1.2. Seguridad de servicios de las aplicaciones en redes públicas. La información involucrada en servicios de aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	**NO**
		A.14.1.3. Protección de transacciones de servicios de aplicaciones. La información involucrada en las transacciones de servicios de aplicaciones se debe proteger para prevenir la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes. La divulgación no autorizada y la duplicación o reproducción de mensajes no autorizados.	**NO**
	A.14.2. Seguridad en los procesos de desarrollo y de soporte.	A.14.2.1. Política de desarrollo seguro. Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas a los desarrollos dentro de la organización.	**NO**
	Objetivo. Asegurar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.	A.14.2.2. Procedimiento de control de cambios en sistemas. Los cambios a los sistemas dentro del ciclo de vida de desarrollo de software y de sistemas a los desarrollos dentro de la organización.	**NO**
		A.14.2.3. Revisión técnica de aplicaciones después de cambios en la plataforma de operaciones. Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y poner a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad organizacionales.	**NO**
		A.14.2.4. Restricciones sobre los cambios de paquetes de software. Se deben desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.	**NO**
		A.14.2.5. Principios de construcción de sistemas de seguros. Se deben establecer, documentar y mantener principios para la organización de sistemas seguros, y aplicarlos a cualquier trabajo de implementación de sistemas de información.	**NO**

		A.14.2.6. Ambiente de desarrollo seguro. Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.	**NO**
		A.14.2.7. Desarrollo contratado externamente. La organización debe supervisar y hacer seguimiento de la actividad de desarrollo de sistemas subcontratados.	**NO**
		A.14.2.8. Pruebas de seguridad de sistemas. Durante el desarrollo se deben llevar a cabo ensayos de funcionalidad de la seguridad.	**NO**
		A.14.2.9. Pruebas de aceptación de sistemas. Para los sistemas de información nuevos, actualizaciones y nuevas versiones se deben establecer programas de ensayo y criterios relacionados.	**NO**
	A.14.3. Datos de ensayo.	A.14.3.1. Protección de datos de ensayo. Los datos de ensayo se deben seleccionar, proteger y controlar cuidadosamente.	**NO**
	Objetivo. Asegurar la protección de los datos usados para ensayos.		
A.15. RELACIONES CON LOS PROVEEDORES.	A.15.1. Seguridad de la información en las relaciones con los proveedores.	A.15.1.1. Política de seguridad de la información para las relaciones con proveedores. Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.	**NO**
	Objetivo. Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.	A.15.1.2. Tratamiento de la seguridad dentro de los acuerdos con proveedores. Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que puedan tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.	**NO**
		A.15.1.3. Cadena de suministro de tecnología de información y comunicación. Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.	**NO**

	A.15.2. Gestión de la prestación de servicios de proveedores.	A.15.2.1. Seguimiento y revisión de los servicios de los proveedores. Las organizaciones deben hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.	**NO**
	Objetivo. Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.	A.15.2.2. Gestión de cambios a los servicios de los proveedores. Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados y la reevaluación de los riesgos.	**NO**
A.16. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.	A.16.1. Gestión de incidentes y mejoras en la seguridad de la información.	A.16.1.1. Responsabilidades y procedimientos. Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.	**NO**
	Objetivo. Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidad.	A.16.1.2. Informe de eventos de seguridad de la información. Los eventos de seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.	**NO**
		A.16.1.3. Informe de debilidades de seguridad de la información. Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que se observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.	**NO**
		A.16.1.4. Evaluación de eventos de seguridad de la información y decisiones sobre ellos. Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.	**NO**
		A.16.1.5. Respuesta a incidentes de seguridad de la información. Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.	**NO**
		A.16.1.6. Aprendizaje obtenido de los incidentes de seguridad de la información. El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debe usar para reducir la posibilidad o el impacto de incidentes futuros.	**NO**

		A.16.1.7. Recolección de evidencia. La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.	**NO**
A.17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DE NEGOCIO.	A.17.1. Continuidad de seguridad de la información	A.17.1.1. Planificación de la continuidad de la seguridad de la información. La organización debe determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastres.	**NO**
	Objetivo. La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.	A.17.1.2. Implementación de la continuidad de la seguridad de la información. La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	**NO**
		A.17.1.3. Verificación, revisión y evaluación de la continuidad de la seguridad de la información. La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información implementados con el fin de asegurar que los válidos y eficaces durante situaciones adversas.	**NO**
	A.17.2. Redundancia	A.17.2.1. Disponibilidad de instalaciones de procesamiento de información. Las instalaciones de procesamiento de información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.	**NO**
	Objetivo. Asegurarse de la disponibilidad de instalaciones de procesamiento de información.		
A.18. CUMPLIMIENTO.	A.18.1. Cumplimiento de requisitos legales y contractuales.	A.18.1.1. Identificación de los requisitos de legislación y contractuales aplicables. Se deben identificar, documentar y mantener actualizados explícitamente todos los requisitos legislativos estatutarios, de reglamentación y contractuales pertinentes, y el enfoque de la organización para cada sistema de información y para la organización.	**NO**

	Objetivo. Evitar violaciones de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.	A.18.1.2. Derechos de Propiedad Intelectual. Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software licenciados.	**NO**
		A.18.1.3. Protección de registros. Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.	**NO**
		A.18.1.4. Privacidad y protección de la información identificable personalmente. Se deben asegurar la privacidad y la protección de la información identificable personalmente, como se exige en la legislación y la reglamentación pertinentes, cuando sea aplicable.	**NO**
		A.18.1.5. Reglamentación de Controles Criptográficos. Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos	**NO**
	A.18.2. Revisiones de seguridad de la información	A.18.2.1. Revisión independiente de la seguridad de la información. El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, la políticas, los procesos y los procedimientos para seguridad de la información se deben revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.	**NO**
	Objetivo. Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimiento organizacionales.	A.18.2.2. Cumplimiento con las políticas y normas de seguridad. Los directores deben revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.	**NO**
		A.18.2.3. Revisión del Cumplimiento Técnico. Los Sistemas de información se deben revisar con regularidad para determinar el cumplimiento con las políticas y normas de seguridad de la información.	**NO**

ANEXO D. RESUMEN ANALÍTICO ESPECIALIZADO RAE

Título de Documento.	AUDITORÍA A LA SEGURIDAD INFORMÁTICA DE LOS SERVICIOS DE TECNOLOGÍAS DE LA INFORMACIÓN EN LA E.S.E HOSPITAL SAN FRANCISCO DE GACHETÁ
Autor	HILARION NOVOA Francisco javier
Palabras Claves	Auditoría, Seguridad Informática, Tecnologías, Magerit usuarios, activos informáticos, ISO/IEC 27001- 27002, E.S.E. Hospital San Francisco de Gachetá, integridad, disponibilidad, confidencialidad, trazabilidad, autenticidad, vulnerabilidades, Wireshark, Kali Linux, Nmap
Descripción El proyecto Auditoría a la seguridad informática de los servicios de tecnologías de la información en la E.S.E. Hospital San Francisco de Gachetá, contempla minimizar el riesgo por pérdida de confidencialidad en los registros de historia clínica e información financiera. Para ello se realiza una auditoría de seguridad informática, integrando pruebas de software, revisión documental, encuestas, listas de chequeo y verificación física con el fin de generar un informe de auditoría que el Hospital pueda poner en marcha a través de un plan de mejoramiento y su posterior seguimiento.	
Fuentes Bibliográficas	SEGURIDAD INFORMÁTICA SMR. Seguridad Informática. [consultado 17 marzo de 2016]. Disponible en internet: https://seguridadinformaticasmr.wikispaces.com/TEMA+1+SEGURIDAD+IFORM%C3%81TICA COSTAS SANTOS, Jesús. Seguridad y alta disponibilidad. 1 ed. Ediciones RA-MA, 2014. p. 10. ECURED. Seguridad informática. [consultado 20 marzo de 2016]. Disponible en: http://www.ecured.cu/Seguridad_Inform%C3%A1tica

	UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Módulo Auditoría de Sistemas. [consultado 25 de marzo de 2016]. Disponible en: http://datateca.unad.edu.co/contenidos/90168/2014MODULO_90168_plantilla_unidad_2.pdf

CONTENIDO

Auditoría de seguridad informática a los servicios de tecnologías de la información de la E.S.E. Hospital San Francisco de Gachetá.

PROBLEMA

En la E.S.E Hospital San Francisco de Gacheta, se maneja una red de datos y servicios de tecnologías de la información, para los diversos servicios administrativos y asistenciales.

El problema que se pretende solucionar en la E.S.E Hospital San Francisco de Gacheta es la pérdida de la confidencialidad de la información, ya que no cuenta con la implementación de procesos de auditoría a la seguridad informática y por ende no existen informes, planes de mejoramiento ni seguimiento a los mismos. Por lo cual existe la posibilidad de perderse la confidencialidad de los registros de historias clínicas y los balances financieros de la entidad.

¿Cómo el proceso de auditoría a los servicios de tecnologías de la información permitirá minimizar la pérdida de la confidencialidad de información financiera y registros de historia clínica en la ESE Hospital San Francisco de Gachetá?

OBJETIVO GENERAL.

Minimizar el impacto de la pérdida de confidencialidad de información financiera y registros de historia clínica a través de la aplicación de una auditoria a la seguridad informática de los servicios de tecnologías de la información en la E.S.E Hospital San Francisco de Gacheta.

OBJETIVOS ESPECÍFICOS.

- Planear la ejecución de la auditoria de seguridad informática, definiendo los métodos, técnicas, procedimientos, plan de pruebas y solicitud de documentos para que la auditoria se lleve a cabo de forma satisfactoria.

- Identificar los riesgos a través de los instrumentos de recolección de información y pruebas que han sido planeadas anteriormente con el fin de medir la probabilidad de ocurrencia y el impacto dentro de la organización.

- Elaborar un dictamen de la auditoría de acuerdo a los hallazgos encontrados para medir los niveles de madurez de la organización.

- Elaborar un informe final de la auditoria con las recomendaciones para que el Hospital establezca el plan de mejoramiento y el sistema de control adecuado.

RESUMEN DE LO DESARROLLADO EN EL PROYECTO.

La planeación de la auditoría permitió desarrollar los siguientes ítems:

Marco referencial: Normatividad, teoría de Auditoría de Seguridad Informática, revisión de la metodología Magerit V3, variables de seguridad informáticas.

Instrumentos de recolección de la información: Entrevista y encuestas

Pruebas de Software: Wireshark, Nmap, Kali Linux

Revisión documental: procesos, procedimientos y manuales

Revisión de aspectos físicos: organización, orden, almacenamiento, limpieza, controles de seguridad

Aplicación de la metodología Magerit: Clasificación de activos informáticos de acuerdo con el inventario de activos, Valoración de los activos informáticos, Identificación de las amenazas, valoraciones, tablas de gestión del riesgo

Informe de auditoría que contemplas las áreas de: Copias de seguridad, infraestructura y redes, acceso físico, firewall, antivirus, contraseñas, ingeniería social, Gestión y Organización.

METODOLOGÍA DE DESARROLLO

Para el desarrollo de la propuesta, se realizaron una serie de actividades que contemplan la realización de una encuesta a algunos funcionarios del hospital, una entrevista al líder de gerencia de la información, un plan de auditoría, un plan de pruebas de software, una revisión de aspectos físicos de la entidad, la clasificación de activos, valoración cuantitativa de los activos, identificación de las amenazas, valoración del riesgo, aplicación de controles y generación de un informe de auditoría.

CONCLUSIONES

- La auditoría de seguridad informática en el Hospital San Francisco de Gachetá ha permitido evidenciar las diferentes vulnerabilidades y amenazas a las que se ven expuestas los activos de información del área administrativa y de historias clínicas del hospital San Francisco de Gachetá por lo que es importante que se tomen medidas para proteger los activos de información y garantizar la continuidad del negocio.

- Utilizando la Metodología MAGERIT V3 se ha realizado la identificación de amenazas y junto con ella la evaluación del riesgo analizando los impactos en cada uno de los activos y se han establecido controles los cuales deben aplicarse según el análisis para proteger los activos informáticos en cada una de las dimensiones en las que se ven afectados.

- El informe de auditoría permitirá al Hospital generar su plan de mejoramiento y su posterior seguimiento, con el fin de garantizar la minimización de la pérdida

de confidencialidad de la información contenida en los registros financieros y de historias clínicas.

RECOMENDACIONES.

Las principales recomendaciones realizadas son:

- Según la auditoría se encuentran diversas amenazas a las que está expuesta la información del Hospital San Francisco de Gachetá, se hace necesario implementar un plan de mejoramiento para el informe de auditoría que se ha descrito en el proyecto y elaborar un seguimiento trimestral al mismo.
- Se debe guardar las copias de seguridad de la información en un lugar diferente a la oficina de gerencia de la información.
- Es importante instalar un UTM con firewall, control de tráfico, seguridad perimetral y generación de reportes de seguridad.
- Es importante instalar un servicio de directorio activo con el fin de centralizar los usuarios y establecer políticas de seguridad.
- Es vital contratar una solución de protección antivirus, con el fin de realizar seguimiento a los incidentes generados,
- Se requiere instalar un control de acceso para administar el ingreso y egreso del personal a la institución.
- Debe de trasladarse la monitorización de el circuito cerrado de televisión al personal de seguridad de la Institución.
- Rediseñar el rack de comunicaciones y organizar el cableado correcta y ordenadamente,
- Establecer un área específica para insumos de mantenimiento y no mezclarlo con la parte documental ni con los registros de backups.
- Organizar el área de Gerencia de la Información en general.

- Documentar todos los procedimientos y protocolos del área de Gerencia de la Información.
- Es necesario que el Hospital San Francisco de Gachetá gestione con los funcionarios del área de gerencia de la información, conocimientos avanzados en seguridad informática y de esa forma sensibilizar y capacitar al personal en general.