DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMATICA BASADO EN LA NORMA ISO/IEC 27001- 27002 PARA EL AREA ADMINISTRATIVA Y DE HISTORIAS CLINICAS DEL HOSPITAL SAN FRANCISCO DE GACHETÁ

EDGAR ALONSO BOJACA GARAVITO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
GACHETA CUNDINAMARCA
2016

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMATICA BASADO EN LA NORMA ISO/IEC 27001-27002 PARA EL AREA ADMINISTRATIVA Y DE HISTORIAS CLINICAS DEL HOSPITAL SAN FRANCISCO DE GACHETÁ

EDGAR ALONSO BOJACA GARAVITO

PROYECTO DE GRADO

Director
PILAR ALEXANDRA MORENO
INGENIERA DE SISTEMAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BASICAS E INGENIERIA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
GACHETA CUNDINAMARCA
2016

Nota de Aceptación:

_____

_____

_____

_____

_____

Firma del Jurado 1

_____

Firma del Jurado 2

GACHETÁ DIA:_____MES:_____AÑO: 2016

En primer lugar dedico este trabajo a Dios por guiarme con su santa voluntad y darme la fortaleza para continuar con mi formación académica.

A mis padres y hermano por su constante apoyo y acompañamiento que día a día me brindan para seguir hacia delante en el proceso de formación académica.

A mi novia Diana por su apoyo constante y acompañamiento los cuales han sido motivantes para no desistir en alcanzar el objetivo de graduarme como especialista.

Finalmente dedico este trabajo a los tutores y compañeros de trabajo de la UNAD que me orientaron y acompañaron durante la especialización. Gracias por ampliar mis conocimientos.

Edgar Alonso Bojacá Garavito

AGRADECIMIENTOS

El autor expresa sus agradecimientos:

A las directivas del hospital San Francisco de Gachetá por permitirnos acceder a la información necesaria la elaboración de este proyecto

A los Magister Salomón González y Pilar Moreno, por el acompañamiento, enseñanzas y sugerencias en la elaboración de este proyecto lo que sin duda ha fortalecido los conocimientos del autor y cuyo resultado sin duda permitirá mejorar el nivel de seguridad informática en el Hospital San Francisco de Gachetá lo que permitirá brindar una mejor atención a los pacientes de la región del Guavio.

A la Universidad Nacional Abierta y a Distancia UNAD, por darme la oportunidad de aumentar mis conocimiento en el campo de la seguridad informática y mejorar mis expectativas laborales y profesionales al obtener el título de especialista

A todas las personas, tutores, compañeros y amigos que con su contribución intelectual, sugerencias y análisis permitieron hacer mejoras en el desarrollo del diseño del sistema de gestión de seguridad informática para el Hospital San Francisco de Gachetá.

CONTENIDO

ANEXOS

pág.

LISTADO DE TABLAS

Pág.

LISTADO DE FIGURAS

Pág.

INTRODUCCIÓN

La seguridad Informática, como tema o eje central de este proyecto hace referencia a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, las cuales garantizan la confidencialidad, trazabilidad, integridad y disponibilidad de la información.

En la actualidad los delitos informáticos son una amenaza latente contra los activos informáticos, para el caso del Hospital San Francisco de Gachetá la información de los pacientes ha tenido una transformación al pasar de papel a archivos digitales en bases de datos los cuales contienen información de historias clínicas de pacientes y archivos con información administrativa y financiera, por lo anterior se requiere implementar un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001- 27002 versión 2013 que mitigue la probabilidad de ocurrencia de delitos informáticos o sucesos similares que alteren la confidencialidad, disponibilidad e integridad de los activos informáticos del área administrativa y de historias clínicas de la entidad hospitalaria.

El proyecto tiene como alcance analizar las vulnerabilidades del sistema informático de la entidad para realizar el diseño de un SGSI que responda a las necesidades de seguridad de información garantizando así la protección total de archivos que al ser alterados pueden generar caos en las historias clínicas de los pacientes, errores en las citas médicas, errores en nómina y desvío de recursos del hospital.

La delimitación se centra en que el desarrollo del proyecto es teórico fundamentado en las experiencias de trabajadores del hospital quienes manifiestan los problemas en la red, infección de virus, acceso sin restricción a los diferentes equipos de cómputo, el manejo de sus correos personales para transferir información administrativa del hospital, falta de backups, por otro lado no es posible hacer pruebas con información real ya que por normas éticas y

morales no podemos tener acceso a información clasificada sin autorización de las altas directivas por lo que el SGSI se aplicara específicamente al área administrativa y de historias clínicas, la infraestructura tecnológica que la soporta y los usuarios del sistema destinado a estas áreas.

En primer lugar se analizan las vulnerabilidades y amenazas informáticas a las que se ve expuesta información digital del Hospital San Francisco de Gachetá aplicando la metodología MAGERIT donde se identifican las causas que generan oportunidad para generar daños a los activos informáticos y se evidencia que la información financiera y administrativa presenta al igual que la información de los pacientes un alto nivel de vulnerabilidad ya que la red del Hospital San Francisco de Gachetá no cuenta con sistemas básicos de protección de información en la red. Una vez se han detectado las vulnerabilidades y amenazas se procede con la determinación de los parámetros y las políticas que se deben implementar en un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001-27002 versión 2013 en el hospital San Francisco de Gachetá.

Finalmente con la información recopilada se procede con el diseño del SGSI de acuerdo a los resultados obtenidos en los análisis de vulnerabilidades y amenazas teniendo en cuenta los controles de la norma ISO/IEC 27001-27002 versión 2013 para el área administrativa y de historias clínicas del hospital San Francisco de Gachetá donde se plantean 4 fases que guiaran el proceso en una futura implementación del presente diseño, lo anterior significa que la propuesta de diseño contempla elementos que le permitirán al Hospital San Francisco de Gachetá proceder con la implementación real a través de una planificación que permita generar una propuesta que una vez ejecutada pueda pasar a una fase de verificación donde gracias al seguimiento que se realice se genere como resultado acciones para mantener y mejorar el sistema de gestión de seguridad informática que mitigue riesgos y vulnerabilidades a los que se exponen los activos de información del área administrativa y de historias clínicas de la entidad hospitalaria.

1. TITULO

Diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001-27002 para el área administrativa y de historias clínicas del hospital san francisco de Gachetá

2. PLANTEAMIENTO DEL PROBLEMA

El municipio de Gachetá Cundinamarca cuenta con un hospital de segundo nivel el cual atiende a una población superior a los 10.000 habitantes incluyendo personas de municipios circunvecinos los cuales encuentran en el hospital San Francisco de Gachetá un apoyo o salvación cuando de curar enfermedades o molestias se trata.

Gracias a los avances de la tecnología el hospital San Francisco de Gachetá ha optado por digitalizar gran cantidad de información que antes se manejaba en formatos a papel los cuales son importantes para su funcionamiento y atención oportuna de pacientes, dicha información es de carácter financiero, administrativo, historial clínico de pacientes, formulas médicas, resultados de exámenes, agendas de citas, médicas entre otros.

Al ser ISO/IEC 27001-27002 versión 2013 un estándar para la seguridad de la información nos orienta o específica los requisitos necesarios para establecer, diseñar, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) lo que lo convierte en nuestra carta de navegación para realizar el estudio y diseño de un sistema de gestión de seguridad de la información en el hospital San Francisco de Gachetá.

Teniendo en cuenta la descripción anterior se plantea la siguiente formulación:
¿Cómo el diseño de un sistema de gestión de seguridad informática SGSI basado en la norma ISO/IEC 27001-27002 versión 2013 permitirá mejorar el nivel de confiabilidad a través del establecimiento de parámetros y políticas de seguridad de la información en el área administrativa y de historias clínicas del hospital San Francisco de Gachetá?

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Establecer parámetros y políticas de seguridad informática mediante el diseño de un sistema de gestión de seguridad de la información SGSI basado en la norma ISO/IEC 27001-27002 versión 2013 para mejorar el nivel de confiabilidad en el área administrativa y de historias clínicas del hospital San Francisco de Gachetá.

3.2 OBJETIVOS ESPECIFICOS

- Determinar los activos informáticos con autorización de la entidad hospitalaria para elegir los dominios de la norma ISO/IEC 27001-27002 versión 2013 que serán aplicados en la evaluación de riesgos.

- Analizar las posibles vulnerabilidades y posibles amenazas informáticas a las que se ve expuesta información digital del Hospital San Francisco de Gachetá aplicando la metodología MAGERIT.

- Determinar los parámetros y las políticas que se deben implementar en un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001-27002 versión 2013 en el hospital san francisco de Gachetá.

- Diseñar el SGSI de acuerdo a los resultados obtenidos en los análisis de vulnerabilidades y amenazas teniendo en cuenta los controles de la norma ISO/IEC 27001-27002 versión 2013 para el área administrativa y de historias clínicas del hospital San Francisco de Gachetá.

4. JUSTIFICACIÓN

Los avances de la tecnología mejoran la calidad de vida, dichos avances han estado orientados a la búsqueda del bien, avances tecnológicos como la computación han sido vitales dentro del desarrollo humano constituyéndose en un pilar de progreso para la civilización humana, un pilar que al derribarse o vulnerarse ocasiona serios inconvenientes a nivel empresarial, social y hasta psicológico, el hospital San Francisco de Gachetá como entidad pública ha optado por digitalizar el 100% de la información de los pacientes de la región del Guavio, dentro de dicha información se encuentran historias clínicas, información financiera y administrativa, citas médicas, medicamentos suministrados, información personal, EPS entre otros.

Por otro lado la información financiera y administrativa presenta al igual que la información de los pacientes un alto nivel de vulnerabilidad ya que la red del Hospital San Francisco de Gachetá no cuenta con sistemas básicos de protección de información en la red, tan solo se evidencia la existencia de un antivirus Avast, y en otros equipos Norton antivirus con licencias de prueba, en otros casos no se cuenta con antivirus y muchos de los equipos no cuentan ni siquiera con niveles de permisos o contraseñas de acceso, por lo que se hace necesario implementar un sistema de gestión de seguridad de la información beneficiando a administrativos y pacientes a través de la protección de su información.

Es importante y urgente realizar la implementación de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001-27002 ISO/IEC 27001-27002 versión 2013 en el Hospital san Francisco de Gachetá en especial para el área administrativa y de historias clínicas ya que las vulnerabilidades saltan a la vista y en cualquier momento se puede generar un ataque con inyección de código, gusanos, virus, entre otros que pondrán en alto riesgo los datos almacenados en la red del hospital afectando seriamente a administrativos

y usuarios de la entidad, de no implementarse dicho sistema la información del área administrativa y de historias clínicas será cada día más vulnerable y propensa a perderse por un ataque informático generando serios daños que afectaran directamente el funcionamiento administrativo de atención de usuarios del hospital lo que traerá como consecuencia demandas de tipo legal por la pérdida de evidencia del uso y dirección de recursos financieros, administrativos y sobre todo por la no atención oportuna a pacientes con diferentes tipos de enfermedad.

5. ALCANCE Y DELIMITACIÓN DEL PROYECTO

El proyecto de diseño de un sistema de seguridad informática basado en la norma ISO/IEC 27001-27002 para el área administrativa y de historias clínicas del hospital San Francisco de Gachetá tiene como alcance analizar las vulnerabilidades del sistema informático de la entidad para realizar el diseño de un SGSI que responda a las necesidades de seguridad de información garantizando así la protección total de archivos que al ser alterados pueden generar caos en las historias clínicas de los pacientes, errores en las citas médicas, generar errores en la nómina y desvío de recursos del hospital.

La delimitación del problema se centra en que el desarrollo del proyecto es teórico fundamentado en las experiencias de trabajadores del hospital quienes manifiestan los problemas en la red, infección de virus, acceso sin restricción a los diferentes equipos de cómputo, el manejo de sus correos personales para transferir información administrativa del hospital, falta de backups, por otro lado no es posible hacer pruebas con información real ya que por normas éticas y morales no podemos tener acceso a información clasificada sin autorización de las altas directivas por lo que el SGSI se aplicara específicamente al área administrativa y de historias clínicas, la infraestructura tecnológica que la soporta y los usuarios del sistema destinado a estas áreas.

Se espera alcanzar el máximo nivel de análisis real de posibles amenazas detectadas, así como de las vulnerabilidades con el fin de generar una propuesta asertiva basado en la norma ISO/IEC 27001-27002 versión 2013 que responda a las necesidades de seguridad informática garantizando satisfactoriamente la protección de los datos del Hospital del municipio de Gachetá durante el periodo de tiempo comprendido entre los años 2015 y 2016 aplicando parámetros y políticas de seguridad informática acordes con la realidad del hospital mejorando el nivel de seguridad de la información.

6. MARCO REFERENCIAL

6.1 ANTECEDENTES

Con relación a los antecedentes se encuentran los siguientes postulados:

Proyecto denominado “Análisis y diseño de un sistema de gestión de seguridad de información basado en la norma ISO/IEC 27001:2005 para una empresa de producción y comercialización de productos de consumo masivo” presentado por Hans Ryan Espinoza Aguinaga en la Pontificia Universidad Católica Del Perú sede Lima (Perú). El proyecto presenta el análisis y diseño del SGSI para la empresa productos de alimentos, el proyecto servirá para determinar la metodología MARGERIT en la identificación de riesgos informáticos.

Proyecto denominado “Planeación y diseño de un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001 – 27002” presentado por José Luis Buenaño Quintana y Marcelo Alfonso Granda Luces en la Universidad Politécnica Salesiana sede Guayaquil en la ciudad de Guayaquil (Ecuador). El proyecto presenta la forma en que mitigan los riesgos asociados con el uso de la información en los sistemas y servicios informáticos dentro de la sede Guayaquil de la Universidad Politécnica Salesiana. Este proyecto servirá para fortalecer el análisis de riesgos de la información y metodología de implementación de la norma ISO/IEC 27001 – 27002.

Proyecto denominado “Plan De Implementación Del SGSI Basado En La Norma ISO 27001:2013” presentado por Robin j. Salcedo B en la Universidad Oberta Catalunya (España). El proyecto presenta el establecimiento de las bases para la implementación de un SGSI (Sistema de Gestión de la Seguridad de la Información) para la empresa ISAGXXX. Este proyecto servirá para identificar los procesos que se utilizan en la implementación del SGSI que serán utilizados en el diseño destinado para el hospital san Francisco de Gachetá.

Proyecto denominado “Diseño De Una Metodología Para La Implementación Del Sistema De Gestión De Seguridad De La Información - SGSI, En El Sector De Laboratorios De Análisis Microbiológicos, Basado En ISO 27001” presentado por Johanna Carolina Buitrago Estrada, Diego Hernando Bonilla Pineda y Carol Estefanie Murillo Varon, el proyecto presenta el Diseño de una metodología de implementación del sistema de gestión de seguridad de la información para empresas del sector de laboratorios de análisis microbiológicos de control de calidad, basado en la ISO 27001. Este proyecto servirá para establecer la metodología que se utilizara en el diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del hospital san francisco de Gachetá.

6.2 MARCO CONTEXTUAL

El proyecto se realizara en el sector salud y se localiza en Colombia, Departamento de Cundinamarca, Municipio de Gachetá, Zona urbana en la E.S.E Hospital San Francisco de Gachetá, más concretamente en la red de sistemas del área administrativa y de historias clínicas donde se proyecta implementar el sistema de seguridad informática basado en la norma ISO/IEC 27001-20072 versión 2013.

✓ **Reseña histórica del Hospital san francisco de Gachetá.** 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 fundación de un Hospital, el cual fue construido en 1905, siendo de carácter particular, con el fin de prestar asistencia social a las personas desposeídas de recursos.[1]

[1] Manuel Darío Guzmán Urrego. Gachetá 400 años, 1993 Bogotá Dc. Colombia.

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 París, 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 1994, 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 y mostraba un atraso general en su tecnología. A partir del año 1986, se inició la modernización del Hospital y se contrató por servicios a 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 Gacheta, II Nivel.[2]

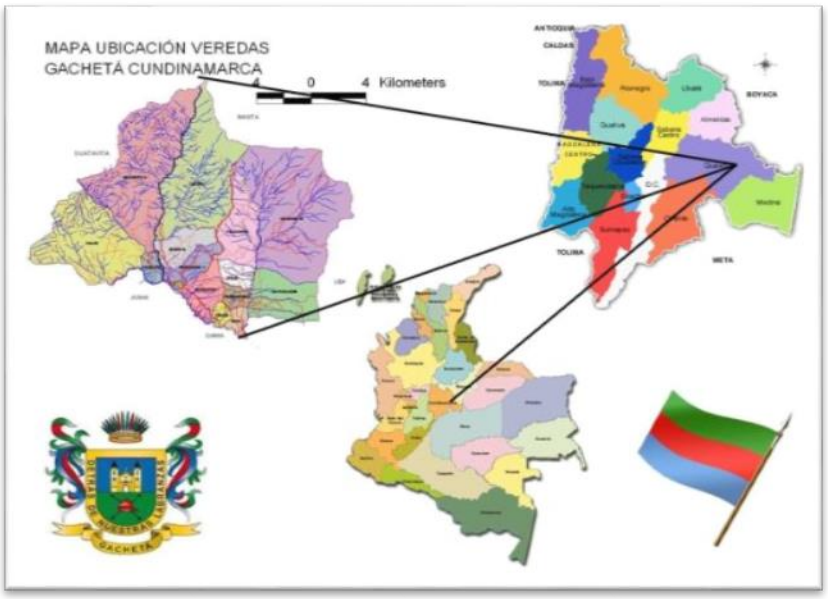
En el año 2003, se inicia el proyecto de habilitación de servicios, en cuanto a su infraestructura tiene unas modificaciones en lo referente a cambios de cubierta, pisos en el área de hospitalización, Terapia Física y Respiratoria y algunos consultorios, adecuación de baños para los usuarios de Consulta Externa, Hospitalización y Urgencias, adecuación del servicio de Urgencias, Sala de Partos y Trabajo de Partos, Central de Esterilización, la 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 y acorde a las exigencias del Ministerio de Protección Social, obras que se encuentran totalmente terminadas en el año 2005.

[2] Manuel Darío Guzmán Urrego. Gachetá 400 años, 1993 Bogotá Dc. Colombia.

En la actualidad cuenta con 38 camas distribuidas en General Adulto, General Pediatría y Obstetricia, servicio de Urgencias las 24 horas, Consulta Externa, Medicina General, Psicología, Nutrición, Fonoaudiología y Optometría, especialistas en Cirugía General, Ginecoobstetricia, Ortopedia, Dermatología, Oftalmología, Otorrinolaringología, Medicina Interna, Pediatría, Urología y Radiología; ayudas Diagnósticas de Endoscopias, Ecografías, Laboratorio Clínico y Rayos X.

✓ **LOCALIZACIÓN.** La entidad se encuentra ubicada en el sector urbano del municipio de Gachetá, cabecera de la provincia del Guavio, Carrera 8ª Salida hacia Bogotá.

Figura 1. Localización y símbolos de Gachetá



Fuente: Manuel Darío Guzmán Urrego. Gacheta 400 años, 1993 Bogotá DC. Colombia

Como punto de referencia puede decirse que Gachetá se localiza a 92 Km de Bogotá Saliendo por la vía a La Calera o por la Autopista norte hasta Briseño, Sopó Guasca, el Páramo, Inspección Sueva y Gachetá, siendo el Hospital la primera edificación que se encuentra al llegar al poblado.

Figura 2. Planta Física Actual E.S.E Hospital San Francisco

Fuente: Autor

✓ **ACTIVIDAD E INFRAESTRUCTURA COMPUTACIONAL.** Su actividad y razón de ser es la atención básica de pacientes con todo tipo de enfermedades prestando el servicio de salud como entidad pública, cuenta con 82 equipos de cómputo de los cuales se encuentran 20 equipos de cómputo destinados a la información administrativo-financiera y 14 equipos destinados a la información de historias clínicas de los pacientes conectados por red LAN a un servidor que cuenta con Windows server sobre los cuales se plantea realizar el diseño de un sistema de seguridad informática basado en la norma ISO/IEC 27001-27002 versión 2013 .

A la fecha no se ha implementado un sistema de seguridad informática, tan solo se evidencia una red para proveer de internet a los equipos que pertenecen a la red informática del hospital.

6.3 MARCO TEÓRICO

✓ **Seguridad informática:** La seguridad Informática, como tema o eje central de este proyecto hace referencia a las características y condiciones de sistemas de procesamiento de datos y su almacenamiento, para garantizar su confidencialidad, integridad y disponibilidad.

La existencia de vulnerabilidades genera la aparición de amenazas, es decir, que al existir una vulnerabilidad, esta puede ser aprovechada por un tercero ´para hacer daño creando situaciones de riesgo que amenacen la integridad de los activos informáticos

Con los avances de la tecnología los ataques informáticos mejoran su efectividad con el fin de afectar a toda costa la información de un individuo, estos ataques mal intencionados que generan algún tipo de afectación se definen como delito informático el cual gracias al " constante progreso tecnológico que experimenta la sociedad, la cual supone una evolución en las formas de delinquir, dando lugar, tanto a la diversificación de los delitos tradicionales como a la aparición de nuevos actos ilícitos".[3] Esta realidad ha originado un debate en torno a la necesidad de distinguir o no los delitos informáticos del resto.

Diferentes autores consideran que los delitos informáticos deben ser tratados como un delito tradicional ya que tras verificar sus efectos se considera que existe gran similitud debido a que los fines son los mismos con la diferencia que los criminales utilizan los medios informáticos para el hecho delictivo.

Tras las amenazas constantes a los diferentes intereses de personas y empresas, las cuales afectan la información confidencial de los usuarios, se ha hecho

[3] Definición de delito informático, internet, http://www.delitosinformaticos.info/delitos_informaticos/definicion.html

necesario establecer el concepto de seguridad informática considerando aspectos como:

“ a) conocer el peligro, b) clasificarlo y c) protegerse de los impactos o daños de la mejor manera posible. Esto significa que solamente cuando estamos conscientes de las potenciales amenazas, agresores y sus intenciones dañinas (directas o indirectas) en contra de nosotros, podemos tomar medidas de protección adecuadas, para que no se pierda o dañe nuestros recursos valiosos. En este sentido, la Seguridad Informática sirve para la protección de la información, en contra de amenazas o peligros, para evitar daños y para minimizar riesgos, relacionados con ella.”[4]

Por esto es importante que en el Hospital san Francisco de Gachetá se analicen las posibles amenazas y vulnerabilidades a las cuales se encuentra expuesta la información para garantizar la confiabilidad, integridad y disponibilidad que permitan el óptimo desempeño del proceso informático organizacional.

Una vez Identificadas las amenazas se puede iniciar con la aplicación de la norma **ISO/IEC 27001-27002 versión 2013** con el fin de garantizar **la seguridad de la información** basándonos en las mejores prácticas, la “norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001-27002 versión 2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

[4]Definición De seguridad informática, internet, https://www.google.com.co/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=bv.105454873,d.dmo

ISO/IEC 27001-27002 versión 2013 : puede ser implementada por cualquier tipo de organización, en este caso particular se implementará en una entidad pública y pequeña como lo es el Hospital San Francisco de Gachetá, Garantizando así la implementación de una metodología elaborada por los mejores especialistas a nivel mundial permitiendo que una vez sea implementado el hospital pueda obtener una certificación por el cumplimiento de la norma ISO 27001-27002.

- ✓ **Metodologías De Gestión De Riesgos MAGERIT:** Gracias a esta metodología creada por el Consejo Superior de Administración Electrónica es posible que las empresas puedan depender de la tecnología y sus avances para sus procesos administrativos obteniendo como resultado el cumplimiento de su razón misional y visional.

Su principal objetivo es el de observar y evaluar el uso de los activos informáticos dentro de una organización para corregir acciones que generen un riesgo contribuyendo así con la mitigación del mismo.

Con esta herramienta se permite a los analistas en seguridad de la información establecer acciones de mejora las cuales deben responder a una serie de controles que contribuyan a la mitigación del riesgo dentro del Hospital San Francisco de Gachetá en el área administrativa y de historias clínicas.

Los activos de información son todos aquellos elementos que utiliza la entidad para la elaboración, edición, transferencia y eliminación de su información, Magerit realiza la clasificación de los mismo de acuerdo a sus características particulares, similitudes o usos elementales lo que permitirá establecer de mejor manera el tratamiento del riesgo para mitigarlo y hacer más segura la infraestructura informática.

En la siguiente tabla se relacionan cada tipo de activos.[5]

Tabla 1. Información de tipos de activos

Tipos de activos	Descripción
Activo de información	Bases de datos, documentación (manuales de usuario, contratos, normativas, etc.)
Software o aplicación	Sistemas de información, herramientas de desarrollo, aplicativos desarrollados y en desarrollo, sistemas operativos, aplicaciones de servidores etc.
Hardware	Equipos de oficina (PC, portátiles, servidores, dispositivos móviles, etc.)
Red	Dispositivos de conectividad de redes (router, swicth, concentradores, etc.)
Equipamiento auxiliar	UPS,
Instalación	Cableado estructurado, instalaciones eléctricas.
Servicios	Conectividad a internet, servicios de mantenimiento, etc.
Personal	Personal informático (administradores, webmaster, desarrolladores, etc.), usuarios finales y personal técnico.

Fuente: UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD Escuela de Ciencias Básicas, Tecnología e Ingeniería Modulo Curso: Sistema de Gestión de la Seguridad de la información SGSI

En primer lugar se debe hacer un levantamiento de la información de los activos informáticos y de allí generar su clasificación de acuerdo a lo establecido por Magerit, este tipo de análisis debe realizarse con la cooperación del personal

[5] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD Escuela de Ciencias Básicas, Tecnología e Ingeniería Modulo *Curso: Sistema de Gestión de la Seguridad de la información SGSI*

responsable del manejo de los activos informáticos y de comunicaciones dentro de la organización.

Dentro del proceso de valoración de Magerit existen 2 escalas valorativas dentro de las cuales se contemplan la cuantitativa y cualitativa, dentro de la cuantitativa se establecen escalas de medidas numéricas para valorar el riesgo clasificándose en:

- ✓ Muy Alto (MA)
- ✓ Alto (A)
- ✓ Medio (M)
- ✓ Bajo (b)
- ✓ Muy bajo (MB)

Según las consideraciones anteriores de metodología Margerit se realizara el respectivo análisis en el Hospital San Francisco de Gachetá a fin de implementar el Diseño de SGSI basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas

Implementación de un SGSI en una organización: Para realizar el proceso de implementación de un SGSI dentro de una organización no se debe esperar a que ocurra un incidente que comprometa la seguridad de los activos informáticos, es importante crear la conciencia de que a medida de que avanza la tecnología y la organización crezca y maneje información confidencial se hace más vulnerable a un ataque por lo que es necesario prever estos ataques diseñando el SGSI estableciendo políticas de control para mitigar el riesgo.

Aspectos se deben considerar al implantar un SGSI: La seguridad de los activos de la información es responsabilidad de todos los integrantes de la organización, como en la mayoría de los casos ocurre existirán algunos funcionarios más comprometidos que otros por lo que es importante concientizar a los diferentes entes organizacionales haciendo relevancia en los perjuicios

económicos, legales, organizaciones entre otros que pueden ser generados como consecuencia de daños a los activos de información.

Tiempo requerido para implantar un SGSI: Los tiempos necesarios para la implementación de un SGSI dependerá de los procesos básicos que tendrá adelantada la empresa donde se piensa implementar, dependerá también de la cooperación y concientización de los funcionarios y también de los procesos administrativos de la empresa y tamaño de la misma, los tiempos se calculan entre 6 meses y un año.

Costo de la implantación de un SGSI: Los costos de implementación dependerán de diferentes variables. La primera se genera cuando la empresa abre licitación para que la implementación la realice otra empresa especializada. Por otro lado es importante analizar si la empresa ya cuenta con personal experto o al menos con conocimientos básicos en el tema, esto sin duda disminuirá costos en contratación adicional. Otra variable es la aplicación o uso de herramientas que ya existan para el análisis de vulnerabilidades, esto disminuirá los costos y tiempo de implementación. Se debe verificar la posibilidad de utilizar herramientas gratuitas o libres para el proceso de análisis.

Finalmente se indica que el costo de implementación del SGSI dependerá del tamaño de la empresa, cuanto más grande sea la empresa, mayor será su costo de implementación, la otra opción que se puede tener en cuenta para reducir costos es hacer la implantación por áreas, factores, dependencias o departamentos según sea la estructura organizacional de la empresa.

Etapas Del Diseño de SGSI: Se deben estudiar los diferentes requisitos de seguridad bajo la norma ISO/IEC 27001 siendo ellos los requisitos o exigencias que debe cumplir la organización para considerarse segura.

Por lo anterior, la ISO 27003 es quien define el análisis de requisitos para implanta un SGSI certificable lo cual es uno de los objetivos para el Hospital San Francisco, donde se define el análisis de requisitos teniendo en cuenta los siguientes ítems:

- Definición de requisitos de seguridad par implementa el SGSI en el hospital

- Identificación de activos dentro de los propósitos alcanzables del SGSI
    - ✓ Clasificación de activos
    - ✓ Identificación de activos

- Evaluar la seguridad de la información en el área administrativa y de historias clínicas del hospital.

- Generar un resumen del estado de seguridad de la información del Hospital San Francisco de Gachetá.

El diseño del SGSI responderá a las necesidades de seguridad y a las políticas establecidas del país donde se implementa, es decir que el SGSI puede variar para organizaciones que tengan sedes en diferentes países pero en esencia deben cumplir con parámetros elementales de mitigación del riesgo. Para tal efecto la normativa ISO 27003, describe características y procedimientos que se deben ejecutar en la etapa de diseño como lo establece su cláusula 9, los cuales se mencionan a continuación:

- Elaboración de las TIC y garantizar seguridad de la información física

- Ejecución de un plan de seguridad de tic y seguridad física.

- Supervisar el diseño del SGSI y verificar los controles para áreas especificas

- Cronograma y pasos para revisiones por la dirección de la entidad
  - ✓ Lista de elementos necesarios para ejecutar la revisión de la gestión.
  - ✓ Pasos a ejecutar para la revisión por parte de la dirección lo que incluye auditoría para realizar la medición de aspectos de la implementación.

- Capacitación sobre la seguridad de activos de información:
  - ✓ Materiales de capacitación pertinentes en seguridad de información
  - ✓ Formación de capacitación en seguridad de información, incluidas las funciones y responsabilidades de cada uno de los funcionarios
  - ✓ Evaluar el proceso de capacitación de seguridad de la información en los funcionarios

- Generar el plan del proyecto SGSI definitiva para realizar la estandarización del plan de ejecución
  - ✓ Establecer los pasos de ejecución del proyecto SGSI definitiva

Se debe definir el alcance y las políticas del SGSI para ello se deben tener en cuenta:

- ✓ Requisitos generales de seguridad
- ✓ Establecimiento y gestión del SGSI
- ✓ Requisitos de documentación

Se debe conseguir la aprobación de la gestión para el inicio de un proyecto de SGSI (Clausula 5 – ISO 27003)

- ✓ Establecer la responsabilidad de la dirección
- ✓ Generar un compromiso de la dirección
- ✓ Garantizar la gestión de recursos necesarios para la elaboración del SGSI

Ejecutar una evaluación del tratamiento de los riesgos (Clausula 8 – ISO 27003)

- ✓ Revisión del SGSI por la dirección
- ✓ Generalidades para la revisión

- ✓ Información para la revisión
- ✓ Resultados de la revisión

Estructuración según la normatividad de gestión de la seguridad. La principal finalidad de las normas de seguridad es la de presentar los lineamientos necesarios para que una entidad como el Hospital San Francisco de Gachetá puedan implantar un sistema de gestión de la seguridad de la información (SGSI).

La implementación del SGSI se debe realizar mediante un proceso organizado que responda al establecimiento de mecanismos que de manera documentada se presenten a todos los integrantes de la organización.

Se debe tener claro que al implementar un SGSI no es posible garantizar en su totalidad la protección de la información de la organización que para este caso es el Hospital San Francisco de Gachetá como lo nombra claramente la ISO en su portal ISO27000.es, —garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.[6]

Las normativas para la creación del SGSI se constituyen en:

- ✓ Normas que vinculen las buenas prácticas para la seguridad de los activos de información que mejoren la calidad de los procedimientos disminuyendo la probabilidad de un incidente contra los activos de información del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá

[6] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD Escuela de Ciencias Básicas, Tecnología e Ingeniería Modulo Curso: Sistema de Gestión de la Seguridad de la información SGSI

- ✓ Normas que deben acatar las empresas en versión documental de cada uno de procesos realizados en la ejecución del SGSI para las organizaciones que deseen certificarse.

6.4MARCO CONCEPTUAL

El sistema de gestión de seguridad de la información SGSI, nace de la necesidad de brindar las garantías mínimas de seguridad en una organización o negocio cuya misión es establecer acciones preventivas en los activos informáticos de la organización contribuyendo así con la mitigación del riesgo.

Con relación al proyecto diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del hospital San Francisco de Gachetá se define dentro de la seguridad de la información preservación de la confidencialidad, la integridad y la disponibilidad; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad.

Según la norma ISO/IEC 27001- 27002 las variables medibles que se identifican dentro del desarrollo del proyecto son:

- ✓ **Confidencialidad**: La variable confidencialidad me permite establecer condiciones para que la información no se ponga a disposición ni se revele a individuos, entidades o procesos no autorizados[7]. En otros términos es la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

[7] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). “Norma Técnica NTC-ISO/IEC Colombiana 27001” Internet http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

✓ **Acuerdos sobre confidencialidad:** Control Se deben identificar y revisar con regularidad los requisitos de confidencialidad o los acuerdos de no-divulgación que reflejan las necesidades de la organización para la protección de la información.

✓ **Integridad**: Se define como la variable de salvaguardar la exactitud y estado completo de los activos mantenimiento de la exactitud y completitud de la información y sus métodos de proceso a través del control.[8] La integridad de la información que se pone a disposición en un sistema de acceso público debe estar protegida para evitar la modificación no autorizada.

✓ **Disponibilidad**: Se define como la variable que establece parámetros para tener acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.[9] Se deben desarrollar e implementar planes para mantener o recuperar las operaciones y asegurar la disponibilidad de la información en el grado y la escala de tiempos requeridos, después de la interrupción o la falla de los procesos críticos para el proyecto.

✓ **Impacto:** Identificar los impactos que la pérdida de confidencialidad, integridad y disponibilidad puede tener sobre estos activos. Analizar y evaluar los riesgos. Valorar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la

[8] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). "Norma Técnica NTC-ISO/IEC Colombiana 27001" Internet http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

[9] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). "Norma Técnica NTC-ISO/IEC Colombiana 27001" Internet http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

pérdida de confidencialidad, integridad o disponibilidad de los activos.[10] La modificación de los procedimientos y controles que afectan la seguridad de la información, según sea necesario, para responder a eventos internos o externos que pueden tener impacto en el SGSI, incluidos cambios a:

1) los requisitos del negocio.
2) los requisitos de seguridad.
3) los procesos del negocio que afectan los requisitos del negocio existentes.
4) los requisitos reglamentarios o legales
5) las obligaciones contractuales.
6) los niveles de riesgo y/o niveles de aceptación de riesgos.

✓ **Probabilidad:** Es la variable medible que me permite establecer el porcentaje de que un incidente de seguridad de la información un evento o serie de eventos de seguridad de la información no deseados o inesperados ocurra en el evento del desarrollo del proyecto, que tienen una probabilidad significativa de comprometer las operaciones del funcionamiento del Hospital en el área administrativa o de historias clínicas amenazando la seguridad de la información.

✓ **Trazabilidad:** Es una variable que nos permite establecer una serie de procedimientos que permiten seguir el proceso de evolución de un producto en cada una de sus etapas que para el desarrollo del proyecto diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá.

✓ **Normativas de Seguridad informática:** Existen diferentes normativas de seguridad que las empresas de hoy implantan para la seguridad de la información.

[10] Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC). “Norma Técnica NTC-ISO/IEC Colombiana 27001” Internet http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Todas estas normativas persiguen los mismos objetivos, ya que están diseñadas para incluir a todas las unidades o departamentos que estructura a la empresa para obtener una seguridad mínima de la información procesada y transferida por el personal que hace parte de ella.[11]

✓ **Código malicioso:** Es un código informático que genera infracciones de seguridad cuya razón de ser es la de dañar un sistema informático. Se trata de un tipo de amenaza cuya solución no siempre puede bloquearse con un software antivirus, por lo general se requiere de un análisis especializado o de utilización de herramientas de mayor profundidad. Según Kaspersky Lab, no toda la protección antivirus puede tratar ciertas infecciones causadas por código malicioso, que es diferente del malware. [12]

✓ **Delito informático:** Acciones que atentan contra la confidencialidad, la integridad y la disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el abuso de dichos sistemas, redes y datos[13]**.** Por lo general un delito informático siempre va contra las políticas de seguridad informática mínimas y vulnera la información confidencial o los activos informáticos de un individuo en particular o de una organización.

✓ **Gusano:** Este tipo de virus por lo general se fundamenta en el funcionamiento de programas que realizan copias de sí mismos, alojándolas en diferentes ubicaciones del ordenador. El objetivo de este malware suele ser

---

[11] UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD Escuela de Ciencias Básicas, Tecnología e Ingeniería Modulo *Curso: Sistema de Gestión de la Seguridad de la información SGSI*

[12] ¿Qué es código malicioso? Internet: http://latam.kaspersky.com/mx/internet-security-center/definitions/malicious-code

[13] Definición de delito informático. Internet http://www.delitosinformaticos.info/delitos_informaticos/definicion.html

colapsar los ordenadores y las redes informáticas, impidiendo así el trabajo a los usuarios. A diferencia de los virus, los gusanos no infectan archivos.[14]

✓ **Hackers:** Un hacker es un individuo experto en alguna rama de la tecnología, a menudo informática, que se dedica a intervenir y/o realizar alteraciones técnicas con buenas o malas intenciones sobre un producto o dispositivo.[15] Muchas de las acciones realizadas por los Hackers constituyen delitos informáticos salvo aquellas en las que se cuenta con autorización previa del dueño de la información o activos informáticos.

✓ **Virus:** Son programas informáticos que tienen como objetivo alterar el funcionamiento del computador, sin que el usuario se dé cuenta. Estos, por lo general, infectan otros archivos del sistema con la intensión de modificarlos para destruir de manera intencionada archivos o datos almacenados en tu computador. Aunque no todos son tan dañinos.[16]

"Las vulnerabilidades de los sistemas informáticos las podemos agrupar en función de:

Diseño

- Debilidad en el diseño de protocolos utilizados en las redes.
- Políticas de seguridad deficiente e inexistente.

Implementación

- Errores de programación.
- Existencia de "puertas traseras" en los sistemas informáticos.

[14] Gusanos. Internet: http://www.pandasecurity.com/colombia/homeusers/security-info/classic-malware/worm/
[15] ¿Qué es un hacker? Internet: http://www.definicionabc.com/tecnologia/hacker-2.php
[16] ¿Qué es un virus informático? Internet: http://www.gcfaprendelibre.org/tecnologia/curso/virus_informaticos_y_antivirus/los_virus_informaticos/1.do

- Descuido de los fabricantes.

Uso

- Mala configuración de los sistemas informáticos.
- Desconocimiento y falta de sensibilización de los usuarios y de los responsables de informática.
- Disponibilidad de herramientas que facilitan los ataques.
- Limitación gubernamental de tecnologías de seguridad.

✓ **Vulnerabilidad del día cero:** Se incluyen en este grupo aquellas vulnerabilidades para las cuales no existe una solución "conocida", pero se sabe cómo explotarla."[17]

✓ **Vulnerabilidad informática:** Definimos Vulnerabilidad como debilidad de cualquier tipo que compromete la seguridad del sistema informático.[18]

✓ **Administrador Informático:** Los **administradores informáticos** controlan y supervisan el procesamiento de trabajo a través de computadoras centrales de gran capacidad. Pueden cargar discos o cintas, y ejecutar programas. Los administradores informáticos también gestionan los errores que se producen en el sistema.[19]

✓ **Amenaza Informática :** Las amenazas básicamente constituyen todo elemento o acción capaz de atacar, afectar o alterar la seguridad de la información.

---

[17] Vulnerabilidades de sistemas informáticos. Internet: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

[18] Vulnerabilidades de un sistema informático. Internet: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

[19] Administrador informatico. Internet: http://www.educaweb.com/profesion/administrador-informatico-55/

✓ **Contraseñas informáticas:** Una *contraseña* (password) en internet, o en cualquier sistema computacional, sirve para autentificar el usuario, o sea, es utilizada en un proceso de ver ificación de la identidad del usuario, asegurando que este es realmente quien dice ser asegurando que no se traten de terceros. [20]

Si otra persona tiene acceso su contraseña, podrá utilizarla para hacerse pasar por otra persona en cualquier actividad que realice en internet. Algunos de los motivos por los cuáles una persona podría utilizar su contraseña son:

- Leer y enviar **e-mails** en su nombre.
- Obtener información sensible de los datos almacenados en su ordenador, tales como **números de tarjetas de crédito**.
- **Esconder su real identidad** y entonces lanzar ataques contra computadoras de terceros.

Por lo tanto, **la contraseña merece consideración especial,** finalmente es de su entera responsabilidad.

✓ **Norma ISO/IEC 27001-27002 versión 2013 :** Representa las mejores prácticas con relación a la seguridad de activos informáticos en las organizaciones, según este marco se pueden establecer controles estandarizados para mitigar el riesgo y mejorar la protección de los activos informáticos.

---

20 Seguridad informática: Todo sobre las Contraseñas. Internet http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Contrasenas-Seguridad-informatica.php

6.5 MARCO LEGAL

Los delitos informáticos constituyen actividades ilegales realizadas por medios informáticos que afectan los intereses de personas, organizaciones públicas y privadas entre otros, este tipo de delitos se enmarcan en figuras tradicionales como lo son hurtos, robos, falsificaciones, fraudes, estafas, perjuicios, sabotajes entre otros. Es importante que tener en cuenta que con los avances de la tecnología se incrementa la posibilidad de cometer delitos informáticos por lo que se ha hecho necesario incrementar controles de carácter legal en Colombia y en el mundo.

Actualmente se considera que no existe una definición clara y concreta para establecer un concepto universal de delito informático debido a que cada nación genera sus propios trámites legales pero se han formulado conceptos respondiendo a realidades nacionales concretas por que no se considera una definición clara de delito informático, sin embargo se establece que delitos ya definidos por la ley se comenten utilizando herramientas informáticas.

Al revisar la historia se encuentra que desde el año 1983 se han realizado estudios para estandarizar las leyes para establecer controles sobre este tipo de delitos siendo ellos:

En el año 1983, la Organización de Cooperación y Desarrollo Económico (OCDE) inicio un estudio de las posibilidades de aplicar y armonizar en el plano internacional las leyes penales a fin de luchar contra el problema del uso indebido de los programas computacionales.[21]

[21] Legislación y Delitos Informáticos - La Información y el Delito. Internet: http://www.segu-info.com.ar/legislacion/

La OCDE público un estudio donde menciona algunos principios legales de delitos habituales como robo, suplantación entre otros donde se utilizan herramientas informáticas y determino que:

- Cualquier comportamiento antijurídico, no ético o no autorizado, relacionado con el procesado automático de datos y/o transmisiones de datos.[22]

- Los delitos informáticos se realizan necesariamente con la ayuda de los sistemas informáticos, pero tienen como objeto del injusto la información en sí misma. [23]

El análisis de la posible ocurrencia de delitos informáticos debe realizarse con el acompañamiento de personal especializado, no solo es asegurar que se cometió un delito, este debe ser sustentado con análisis forense, evidencia digital entre otros que garanticen la ocurrencia del hecho, de lo contrario se podría incurrir en calumnia o desprestigio de una persona por lo que se recomienda asesorarse antes de proceder con alguna acusación.

Basándose en lo anterior la legislación de las leyes contra delitos informáticos debe tener en cuenta los siguientes aspectos:

- ✓ En ningún momento los activos informáticos atentan contra el hombre, es este quien utiliza a los activos de información para cometer el crimen.

- ✓ Los activos de información no son quienes atentan contra la intimidad de los usuarios, es el hombre quien utiliza los medios informáticos para atentar contra la intimidad e información del otro.

---

[22] Definición elaborada por un Grupo de Expertos, invitados por la OCDE a París en Mayo de 1993.

[23] CARRION, Hugo Daniel. Tesis "Presupuestos para la Punibilidad del Hacking". Julio *2001.*http://www.delitosinformaticos.com/tesis.htm

- ✓ La informática no representa un peligro para la humanidad, es el uso de la computación por parte de individuos mal intencionados lo que representa una amenaza.

Dentro de las leyes nacionales que aplican a este proyecto para proteger los activos informáticos del Hospital San Francisco de Gachetá se citan a continuación las siguientes:

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.

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

7. MARCO METODOLÓGICO

7.1 METODOLOGÍA DE INVESTIGACIÓN

Para el desarrollo de la propuesta de diseño de un sistema de seguridad informática basado en la norma ISO/IEC 27001-27002 en el Hospital San Francisco De Gachetá se propone la **Investigación exploratoria** ya que es considerada como el primer acercamiento científico a un problema. Se utiliza cuando el proceso no ha sido investigado con anterioridad o no se han generado situaciones donde se hubiera ameritado un estudio en el pasado, por lo que aplica para este caso ya que la problemática en lo relacionado con el sistema de gestión de seguridad informática no ha sido estudiada en el Hospital San Francisco lo que genera que las condiciones para la solución del problema.

Para el caso específico del diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del 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.

Por lo anterior se debe realizar una **investigación exploratoria con enfoque cuantitativo** ya que nunca se ha realizado una exploración de la problemática en seguridad informática del hospital y para ello se requiere realizar medición de diferentes variables de seguridad informática.

7.2 UNIVERSO Y MUESTRA

- **Universo**

El universo del proyecto diseño de un sistema de seguridad informática basado en la norma ISO/IEC 27001-27002 versión 2013 en el Hospital San Francisco

De Gachetá es el personal de la institución que tiene acceso a los equipos de cómputo los cuales son utilizados en las labores diarias del funcionamiento del hospital en los diferentes campos de acción o departamentos en los cuales se divide la entidad.

- **Muestra**

La muestra está definida por los usuarios de los equipos de cómputo del área administrativa y de historias clínicas del Hospital San Francisco de Gacheta, 20 equipos de cómputo destinados a la información administrativo-financiera y 14 equipos destinados a la información de historias clínicas para un total de 34 equipos de cómputo y la misma cantidad de usuarios.

7.3 INSTRUMENTOS DE RECOLECCIÓN DE INFORMACIÓN

Con el fin de realizar la efectiva recolección de información para el diseño de un sistema de seguridad informática basado en la norma ISO/IEC 27001-27002 versión 2013 en el Hospital San Francisco De Gachetá se utilizaran los siguientes instrumentos:

- Entrevista a las personas encargadas de los equipos de computo
- Lista de chequeo a la red actual para identificar fallas y vulnerabilidades

Se espera que al aplicar estos tres instrumentos se determinen las causas reales de vulnerabilidades y amenazas a las que se expone la información de la entidad generando un diseño pertinente de seguridad informática basado en la norma ISO/IEC 27001-27002 versión 2013. .

7.4 METODOLOGÍA DE DESARROLLO

Para el desarrollo satisfactorio de la propuesta es necesario realizar 4 pasos fundamentales los cuales nos llevarán al de diseño de un sistema de seguridad

informática basado en la norma ISO/IEC 27001-27002 versión 2013 en el Hospital San Francisco De Gachetá, los pasos para la metodología del desarrollo son:

- **Determinar los activos informáticos de la empresa para elegir los dominios de la norma ISO/IEC 27001-27002 versión 2013 que serán aplicados en la evaluación de riesgos.** Es importante determinar en primer lugar los activos informáticos de la empresa esto permitirá elegir los dominios de la norma ISO/IEC 27001-27002 versión 2013 que serán aplicados en la evaluación de riesgos lo que traerá como consecuencia la disminución del riesgo informático y la aplicación asertiva de los dominios de la norma a utilizar gracias a que se identifican las características técnicas de los equipos y la red informática de los cuales hacen parte, su función y cantidad real que hacen uso de estos recursos por lo cual se propone:

✓ Realizar visita de reconocimiento de la red para identificar los activos informáticos.

✓ Entrevistar al o los encargados del soporte de la red informática.

- **Analizar las posibles vulnerabilidades y posibles amenazas informáticas a las que se ve expuesta información digital de hospital san francisco de Gachetá aplicando la metodología MAGERIT.** Determinados los activos de la entidad se realiza un análisis de las vulnerabilidades y amenazas a las que se ve expuesta información digital de hospital san francisco de Gachetá se procede a analizar las posibles vulnerabilidades a través de:

✓ Implementación de la metodología MAGERIT en la entidad hospitalaria.

- **Determinar los parámetros y políticas que se deben implementar en un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001-27002 versión 2013 en el hospital san francisco de Gachetá.**

Tras realizar el análisis de las amenazas y vulnerabilidades se tiene ya determinadas las acciones a realizar por lo que se pueden determinar los controles que deben aplicarse para el diseño de un sistema de seguridad informática basado en la norma ISO/IEC 27001-27002 versión 2013 en el Hospital San Francisco de Gachetá para lo cual se propone:

- Seleccionar los dominios de acuerdo a la normal que sean pertinentes y que respondan a las necesidades de seguridad de la entidad hospitalaria.

- Seleccionar los controles a implementar de acuerdo a la normal que sean pertinentes y que respondan a las necesidades de seguridad de la entidad hospitalaria.

- **Diseñar el SGSI de acuerdo a los resultados obtenidos en los análisis de vulnerabilidades y amenazas teniendo en cuenta los parámetros de la norma ISO/IEC 27001-27002 versión 2013 para el área administrativa y de historias clínicas del hospital San Francisco de Gachetá aplicando políticas de seguridad informática aplicables a la realidad de la organización**. Esta es quizá la parte fundamental del trabajo ya que es aquí donde se concibe la realización del objetivo principal porque al analizar amenazas y vulnerabilidades y tomadas las decisiones sobre controles a implementar se procede al diseño del SGSI de acuerdo a los resultados obtenidos en los análisis de vulnerabilidades y amenazas teniendo en cuenta los controles de la norma ISO/IEC 27001-27002 versión 2013 para el Hospital San Francisco de Gachetá por lo cual se realiza:

  - Diseño de SGSI para la entidad según las necesidades, vulnerabilidades y amenazas detectadas.

  - Elaboración de política para mantener la integridad, confiabilidad y disponibilidad de la información.

8. RECURSOS NECESARIOS PARA EL DESARROLLO

Los recursos necesarios para el diseño de un sistema de seguridad informática basado en la norma ISO/IEC 27001-27002 versión 2013 en el Hospital San Francisco De Gachetá son los siguientes:

- **Humanos**: El recurso humano constituye el elemento vital para la implementación de sistema de seguridad informática basado en la norma ISO/IEC 27001-27002 versión 2013 en el Hospital San Francisco De Gachetá, es importante que este recurso humano cuente en primera medida con personal capacitado y certificado en seguridad informática, complementando esto es importante que los funcionarios del área administrativa y de historias clínicas junto con la gerencia sean un recurso humano importante en lo referente a la concientización que junto con el área departamento de sistemas conformen un equipo que permita mitigar el riesgo y proteger la información de pacientes del hospital siendo este último la razón de ser del hospital

- **Físicos:** Los recursos físicos constituyen uno de los elementos a proteger dentro del SGSI, además y gracias a estos se permite generar un mejor análisis de la situación de seguridad teniendo en cuenta la usabilidad de estos dentro de los procesos de producción realizado por los funcionarios, es importante que se motive al personal en su cuidado, mantenimiento y protección por lo cual es vital que el departamento de sistemas mantenga sus inventarios actualizados para evitar la posible adquisición de equipos que por sus características ya hacen parte de los activos informáticos del hospital.

Tabla 2 Recursos físicos

RECURSO FISICO	DESCRIPCIÓN	VALOR/CANTIDAD
Equipos de computo	20 equipos de cómputo destinados a la información administrativo-financiera y 14 equipos destinados a la información de historias clínicas de los pacientes	34
Funcionarios capacitados	20 funcionarios del departamento administrativo y financiero y 14 del área de historias clínicas capacitados en nociones de seguridad informática necesarias para el desempeño de sus funciones.	34
Ingeniero electrónico/ sistemas	Persona con conocimientos en redes, sistemas operativos y seguridad informática	1
Equipos de red	Servidor, router, switch	4
Bibliografía consultada	Consultas de escritos de expertos en internet, leyes y escritos	15

Fuente: autor

- **Técnicos**:

Es necesario establecer las alternativas técnicas elegidas y las tecnologías a utilizar para el diseño de un sistema de seguridad informática basado en la norma ISO/IEC 27001-27002 versión 2013 en el Hospital San Francisco De Gachetá.

No olvidar que al momento de implementar un SGSI se incurrirá en una inclusión de nuevas soluciones tecnológicas, esto no siempre garantiza una protección total, además estas innovaciones probablemente choquen con la tecnología previamente implementada en el área administrativa y de historias clínicas del hospital por lo que se debe valorar los elementos con que cuenta el hospital y realizar adaptaciones para crear una infraestructura tecnológica que responda a las necesidades de la entidad.

Tabla 3. Recursos técnicos

Recurso técnico	Descripción	Cantidad
Equipos de computo	20 equipos de cómputo destinados a la información administrativo-financiera y 14 equipos destinados a la información de historias clínicas de los pacientes	34
Equipos de red	Servidor, router, switch, firewall que permitirán mejorar la calidad de seguridad de la información	7
Energía eléctrica – UPS de respaldo	Instalación trifásica regulada con UPS de respaldo	1
Protección contra incendios	Equipamiento de incendios adecuado que responda a las necesidades de respuesta ante una emergencia propiciada por fuego	3
Controles de acceso físicos	Controles de acceso a las instalaciones de administración financiera y de historias clínicas con restricciones y registros de la	3

	persona que ingresa y/o sale del espacio protegido	
Licencias de sistemas operativos	Verificación de la originalidad de las licencias de los sistemas operativos instalados en servidores y los 34 equipos de cómputo.	36
Licencias de antivirus de alto nivel de seguridad	Verificación de la originalidad de las licencias de antivirus instalados en servidores y los 34 equipos de cómputo y su pertinencia de respuesta a una posible infección	36

Fuente: Autor

9. METOLOGIA MAGERIT APLICADO AL HOSPITAL SAN FRANCISCO DE GACHETA

9.1 INVENTARIO DE ACTIVOS

La elaboración del inventario de activos del Hospital San Francisco de Gachetá se basa en todos los elementos que la institución posee para el tratamiento de la información (hardware, software, recurso humano, etc.).

Para generar el proceso del inventario de los activos de información, en primer lugar se revisan los listados facilitados por el departamento de sistemas y se procede a identificar la existencia de cada uno de los equipos, se encontró que en algunos casos aún se relacionaban equipos que ya habían sido dados de baja y por otro lado existían equipos sin relacionar, todo esto se realiza en compañía del coordinador del departamento de sistemas.

Una vez se finalizan la revisión de la información versus los equipos que existen en el área administrativa y de historias clínicas se determinó que para el caso del Hospital San Francisco De Gachetá se encuentra el siguiente inventario de activos relacionado en la tabla de acuerdo a su clasificación:

Tabla 4. Inventario de activos de acuerdo a su clasificación

Clasificación de activos	***Descripción***
Activo de información	• Bases de datos de CNT módulo de pacientes. • Bases de datos financieras de CNT modulo tesorería, facturación y contable • Bases de datos y documentos administrativos CNT inventarios
Software o aplicación	• Microsoft Windows 7Professional - licencia asociada a cada PC 34 en total

	• Windows server • Google Crome • Mozilla Firefox • 34 licencias de Office 2013 • CNT programa de gestión administrativa, (programa eje del funcionamiento del hospital) • CNT Modulo Pacientes.(historias clínicas) • SISGEHOS (Sistema de Gestión Hospitalaria, apoyo a CNT)
Hardware	• 34 computadores de escritorio • 1 servidor local
Red	• Router • 3 Swicth
Equipamiento auxiliar	• Planta de energía eléctrica • Cableado estructurado • Instalaciones eléctricas trifásicas no reguladas.
Servicios	• Conectividad a internet de 2Mb. • Servicios de mantenimiento infraestructura física.
Personal	• Un ingeniero de sistemas (apoyo a gestión de infraestructura tecnológica coordinador del departamento de sistemas) • Un tecnólogo de sistemas (apoyo a gestión de infraestructura tecnológica apoyo del departamento de sistemas) • 34 usuarios finales.

Fuente: autor

La anterior clasificación nos permitirá establecer una valoración de los activos teniendo en cuenta la metodología Magerit, también nos permitirá determinar posibles dominios y controles, los cuales en adelante se analizarán para crear políticas de seguridad que contribuyan a la mitigación del riesgo.

Teniendo en cuenta el inventario de los activos de información del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá se han establecido como primer paso unos candidatos de los dominios de la norma ISO/IEC 27001-27002 versión 2013 ya que posiblemente respondan a las necesidades de mejora del nivel de seguridad informática para cada uno de los equipos del área administrativa y de historias clínicas del Hospital ya que podrían contrarrestar las posibles amenazas que se presentan para cada uno de los activos anteriormente mencionados constituyéndose en medidas previas para la materialización del riesgo el cual será analizado más adelante utilizando la metodología Magerit.

Los dominios de la norma ISO/IEC 27001-27002 versión 2013 que serán aplicados en la evaluación de riesgos son:

- ✓ Organización de la Seguridad de la Información.
- ✓ Seguridad de los Recursos Humanos.
- ✓ Gestión de los Activos.
- ✓ Control de Accesos.
- ✓ Seguridad Física y Ambiental.
- ✓ Seguridad de las Operaciones: procedimientos y responsabilidades, protección contra malware, resguardo, registro de actividad y monitorización, control del software operativo; gestión de las vulnerabilidades técnicas.
- ✓ Seguridad de las Comunicaciones: gestión de la seguridad de la red, gestión de las transferencias de información.
- ✓ Gestión de Incidencias que afectan a la Seguridad de la Información: gestión de las incidencias que afectan a la seguridad de la información, mejoras.
- ✓ Aspectos de Seguridad de la Información para la Gestión de la Continuidad del Negocio: continuidad de la seguridad de la información, redundancias.
- ✓ Conformidad: conformidad con requisitos legales y contractuales, revisiones de la seguridad de la información.

9.1.1 Valoración de los activos. La metodología Magerit contempla sus diferentes pilares como son la confidencialidad, la integridad, disponibilidad, y trazabilidad para realizar la valoración de los activos informáticos de una organización.

Un activo se valora en las siguientes dimensiones:

• **Confidencialidad**: ¿Cuál sería el daño si lo conociera quien no debe? Esta valoración se debe aplicar y es válida para los datos del Hospital San Francisco.

• **Integridad**: ¿Cuál es el perjuicio si el activo estuviera dañado o corrupto? Esta valoración se aplica a los datos, ya que estos pueden ser manipulados, total o parcialmente falsos o, incluso, faltar datos del Hospital San Francisco.

• **Disponibilidad**: ¿Cuál es el perjuicio al no tenerlo o no poder utilizarlo? Esta valoración se aplica a los diferentes servicios del Hospital San Francisco.

•**Autenticidad:** Los activos de información del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá los crean, editan y los funcionarios de estas oficinas, tan solo podrá solicitar una revisión o manipulación de los mismos la gerencia del Hospital y en todo momento se contará con el acompañamiento de los funcionarios del departamento de sistemas.

• **Trazabilidad:** ¿Cuál sería el daño al no saber a quién se le presta tal servicio? O sea, ¿quién hace qué y cuándo? Esta aplica de manera directa al acceso a los datos por lo que para el caso del Hospital San Francisco surge otra pregunta: ¿Cuál sería el daño al no saber quién accede a qué datos y qué hace con ellos?

La metodología Margerit también contempla dos tipos de valoraciones, cualitativa y cuantitativa. La primera hace referencia a calcular un valor a través de una escala cualitativa, donde se valora el activo de acuerdo al impacto que puede

causar en el hospital con respecto a su daño o perdida, en consecuencia la escala se refleja en:

- ✓ Extremo
- ✓ Muy Alto (MA)
- ✓ Alto (A)
- ✓ Medio (M)
- ✓ Bajo (b)
- ✓ Despreciable (MB)

Tabla 5. Valoración de activos por criterio

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	Irrelevante a efectos prácticos

Fuente: Magerit v3 libro2 catálogo de elementos.

Tabla 6. Criterios de valoración

CRITERIOS DE VALORACIÓN		
Valor	**Criterio**	
10	10.si	**[si] Seguridad:** Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
	10.olm	**[olm] Operaciones:** Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística.
	10.lbl	**[lbl.nat] Información clasificada (nacional):** Secreto
9	9.lro	**[lpo] Obligaciones legales :** probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
	9.si	**[si] Seguridad:** probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
	9.cei.d	**[cei] Intereses comerciales o económicos:** causa de pérdidas económicas excepcionalmente elevadas

	9.cei.d	**[cei] Intereses comerciales o económicos:** causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.da	**[da] Interrupción del servicio:** Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.olm	**[olm] Operaciones:** Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
	9.lg.b	**[lg] Pérdida de confianza (reputación):** Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general.
	9.lbl	**[lbl.nat] Información clasificada (nacional):**Reservado
8	8.lbl	**[lbl.nat] Información clasificada (nacional) :**Confidencial
7	7.si	**[si] Seguridad:** probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves.
	7.cei.c	**[cei] Intereses comerciales o económicos:** causa de graves pérdidas económicas
	7.da	**[da] Interrupción del servicio:** Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.olm	**[olm] Operaciones:** Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
	7.lg.b	**[lg] Pérdida de confianza (reputación):**Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
	7.lbl	**[lbl.nat] Información clasificada (nacional):** Confidencial
6	6.pi1	**[pi] Información de carácter personal:** probablemente afecte gravemente a un grupo de individuos
	6.lbl	**[lbl.nat] Información clasificada (nacional):** Difusión limitada
5	5.pi1	**[pi] Información de carácter personal:** probablemente afecte gravemente a un individuo
	5.da	**[da] Interrupción del servicio:** Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.lbl	**[lbl.nat] Información clasificada (nacional):** Difusión limitada
	5.adm	**[adm] Administración y gestión:** probablemente impediría la operación efectiva de más de una parte de la Organización
4	4.pi1	**[pi] Información de carácter personal:** probablemente afecte a un grupo de individuos
	4.lbl	**[lbl.nat] Información clasificada (nacional):** Difusión limitada
	3.pi1	**[pi] Información de carácter personal:** probablemente afecte a un individuo

3	3.si	**[si] Seguridad:** probablemente sea causa de una disminución en la seguridad o dificulte la investigación de un incidente
	3.cei.e	**[cei] Intereses comerciales o económicos:** constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
	3.da	**[da] Interrupción del servicio:** Probablemente cause la interrupción de actividades propias de la Organización
	3.olm	**[olm] Operaciones:** Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
	3.lg	**[lg] Pérdida de confianza (reputación):** Probablemente afecte negativamente a las relaciones internas de la Organización.
	3.lbl	**[lbl.nat] Información clasificada (nacional):** Difusión limitada
2	2.pi1	**[pi] Información de carácter personal:** pudiera causar molestias a un individuo.
	2.cei.b	**[cei] Intereses comerciales o económicos:** de bajo valor comercial
	2.lg	**[lg] Pérdida de confianza (reputación):** Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.pi1	**[pi] Información de carácter personal:** pudiera causar molestias a un individuo
	1.si	**[si] Seguridad:** pudiera causar una disminución en la seguridad o dificultar la investigación de un incidente
	1.cei.b	**[cei] Intereses comerciales o económicos:** de pequeño valor comercial
	1.da	**[da] Interrupción del servicio:** Pudiera causar la interrupción de actividades propias de la Organización
	1.olm	**[olm] Operaciones:** Pudiera disminuir la eficacia o seguridad de la misión operativa o logística (alcance local)
	1.lg	**[lg] Pérdida de confianza (reputación):** Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	1	No afecta la seguridad de las personas
	2	Sería causa de inconvenientes mínimos a las partes afectadas
	3	Supondría perdidas económicas mínimas
	4	No supondría daño a la reputación de la organización

Fuente: Autor

Tabla 7. Valoración de activos

VALORACIÓN DE ACTIVOS											
Nombre del activo	**Disponibilidad**		**Integridad**		**Confidencialidad**		**Autenticidad**		**Trazabilidad**		**Valor total**
	Valor	**Justificación**	**Valor**	**Justificación**	**Valor**	**Justificación**	**Valor**	**Justificación**	**Valor**	**Justificación**	
Bases de datos de CNT módulo de pacientes.	10	si	9	Olm	9	lg	9	si	9	Olm	9
Bases de datos financieras de CNT modulo tesorería, facturación y contable.	10	si	9	Olm	9	lg	9	si	9	Olm	9
Bases de datos y documentos administrativos CNT inventarios	9	si	9	Olm	9	lg	9	si	9	Olm	9
Microsoft Windows 7Professional	9	da	9	Olm	9	lbl	9	da	9	Olm	9
Windows server	10	si	9	Olm	9	lbl	9	da	9	Olm	9
Google Crome	7	da	7	Olm	5	Lbd	5	pi1	7	cei.c	6
Mozilla Firefox	7	da	7	Olm	5	Lbd	5	pi1	7	cei.c	6
34 Licencias de office 2013	7	da	7	Olm	5	Lbd	5	pi1	7	cei.c	6
CNT modulo pacientes. (historias clínicas)	10	si	10	Olm	10	lbl	10	si	9	Iro	10
SISGEHOS	10	si	9	Olm	9	lg	9	si	9	Olm	9
CNT programa de gestión	10	si	10	Olm	10	lbl	10	si	9	Iro	10

administrativa, (programa eje del funcionamiento del hospital)											
34 puestos de trabajo (computadores)	5	da, adm	7	Olm	5	pi1	5	pi1	7	cei.c	6
1 servidor local	9	si	9	Olm	9	lg.b	10	si	9	lro	9
Router	5	da, adm	7	Olm	5	pi1	5	pi1	7	cei.c	6
3 Swicth	5	da, adm	7	Olm	5	pi1	5	pi1	7	cei.c	6
Planta de energía eléctrica	5	da	7	olm	3	lg	5	da	3	cei.e	5
Cableado estructurado	5	da	7	olm	3	lg	5	da	3	cei.e	5
Instalaciones eléctricas trifásicas no reguladas.	5	da	7	olm	3	lg	5	da	3	cei.e	5
Conectividad a internet 2Mb.	7	da	7	Olm	5	Lbd	5	pi1	7	cei.c	6
Servicios de mantenimiento infraestructura fisica.	7	da	7	olm	7	lg	7	olm	7	da	7
Ingeniero de sistemas	9	da, lro	7	olm,cei.c	10	lg	9	si	9	cei	9
Tecnólogo en sistemas	9	da, lro	7	olm,cei.c	9	lg	9	si	9	cei	9
34 usuarios finales.	7	si, da	7	cei.c	5	lbl	9	si	9	cei	7

Fuente: Autor

En cuanto a la valoración cuantitativa es necesario también que se realice una escala de valores que permita al hospital estimar su valor que no sólo es el costo que tuvo inicialmente el activo, también se debe tener en cuenta variables de valor inicial, costo de reposición, costo de configuración, costo de uso del activo y valor de perdida de oportunidad.

Para el caso del hospital San Francisco de Gachetá se ha establecido la siguiente escala de valores cuantitativos:

Tabla 8. Valoración cuantitativa de los activos

Valoración cualitativa	Escala de valor cuantitativo expresado en millones	ACTIVO
Alto (A)	8 <valor> 15	• SERVIDOR LOCAL. • CNT programa de gestión administrativa, (programa eje del funcionamiento del hospital).
Medio (M)	2 <valor> 7	• Equipos de computo • Licencia de Software de herramientas ofimáticas • Licencias de Microsoft Windows 7Professional • Licencia de Software adicional, winrar, acrobat, entro otros.
Bajo (B)	0 <valor> 2	• Router • Swicth

Fuente: Autor

9.1.2 Amenazas (identificación y valoración)

Las amenazas son situaciones que dañan o deterioran directa o indirectamente cualquier tipo de activo informático dentro de la organización afectándolo en los 4 pilares de seguridad informática constituyéndose en un daño que puede sufrir el sistema de la organización.

Con relación a la valoración de las amenazas para el caso del Hospital San Francisco de Gachetá tenemos los siguientes aspectos:

Tabla 9. Clasificación de amenazas encontradas en el Hospital San Francisco de Gachetá.

CLASIFICACIÓN	TIPO DE AMENAZA
Desastres naturales	• Fuego • Daños por agua • Desastres naturales
De origen industrial	• Fuego • Daños por agua • Desastres industriales • Contaminación electromagnética • Avería de origen físico o lógico • Corte del suministro eléctrico • Condiciones inadecuadas de temperatura o humedad • Fallo de servicios de comunicaciones • Interrupción de otros servicios o suministros esenciales • Degradación de los soportes de almacenamiento de la información
Errores y fallos no intencionados	• Errores de los usuarios • Errores del administrador • Errores de configuración • Difusión de software dañino • Fugas de información • Alteración de la información • Introducción de falsa información • Degradación de la información • Destrucción de la información • Divulgación de información

	• Vulnerabilidades de los programas (software) • Errores de mantenimiento / actualización de programas (software) • Errores de mantenimiento / actualización de equipos (hardware) • Caída del sistema por agotamiento de recursos • Pérdida de equipos • Indisponibilidad del personal
Ataques deliberados	• Manipulación de la configuración • Suplantación de la identidad del usuario • Abuso de privilegios de acceso • Acceso no autorizado • Análisis de tráfico • Repudio • Modificación de información • Introducción de falsa información • Corrupción de la información • Destrucción de la información • Divulgación de información • Denegación de servicio • Robo de equipos • Extorsión • Ingeniería social (picaresca)

Fuente: Autor

Tabla 10. Valoración de amenazas por tipo de activos

TIPO DE ACTIVO A PROTEGER	CRITERIO DE VALORACIÓN DE ACTIVOS	VALOR	AMENAZAS
Activo de información	Daño muy grave a la	10	• Fuego • Daños por agua • Desastres naturales • Desastres industriales • Contaminación electromagnética • Avería de origen físico o lógico • Condiciones inadecuadas de temperatura o humedad • Degradación de los soportes

	organización		de almacenamiento de la información • Errores de los usuarios • Errores del administrador • Difusión de software dañino • Fugas de información • Alteración de la información • Introducción de falsa información • Destrucción de la información • Divulgación de información • Pérdida de equipos • Manipulación de la configuración • Suplantación de la identidad del usuario • Abuso de privilegios de acceso • Acceso no autorizado • Modificación de información • Corrupción de la información • Denegación de servicio • Robo de equipos • Ingeniería social (picaresca)
Software o aplicación	Daño grave a la organización	9	• Fuego • Daños por agua • Desastres naturales • Desastres industriales • Contaminación electromagnética • Avería de origen físico o lógico • Corte del suministro eléctrico • Fallo de servicios de comunicaciones • Interrupción de otros servicios o suministros esenciales • Errores de los usuarios • Errores del administrador • Errores de configuración

			• Difusión de software dañino • Vulnerabilidades de los programas (software) • Errores de mantenimiento / actualización de programas (software) • Manipulación de la configuración • Suplantación de la identidad del usuario • Abuso de privilegios de acceso • Repudio • Denegación de servicio • Robo de equipos
Hardware	Daño grave a la organización	8	• Fuego • Daños por agua • Desastres naturales • Desastres industriales • Contaminación electromagnética • Avería de origen físico o lógico • Corte del suministro eléctrico • Condiciones inadecuadas de temperatura o humedad • Interrupción de otros servicios o suministros esenciales • Degradación de los soportes de almacenamiento de la información • Errores de los usuarios • Errores del administrador • Errores de configuración • Errores de mantenimiento / actualización de equipos (hardware) • Pérdida de equipos • Indisponibilidad del personal • Manipulación de la configuración • Robo de equipos

			• Extorsión • Ingeniería social (picaresca)
Red	Daño importante a la organización	6	• Fuego • Daños por agua • Desastres naturales • Desastres industriales • Contaminación electromagnética • Avería de origen físico o lógico • Corte del suministro eléctrico • Condiciones inadecuadas de temperatura o humedad • Fallo de servicios de comunicaciones • Interrupción de otros servicios o suministros esenciales • Degradación de los soportes de almacenamiento de la información • Caída del sistema por agotamiento de recursos • Pérdida de equipos • Indisponibilidad del personal • Manipulación de la configuración • Acceso no autorizado • Análisis de tráfico • Repudio • Denegación de servicio • Robo de equipos
Equipamiento auxiliar	Daño importante a la organización	5	• Fuego • Daños por agua • Desastres naturales • Desastres industriales • Avería de origen físico o lógico • Corte del suministro eléctrico • Condiciones inadecuadas de temperatura o humedad

			• Errores de los usuarios • Errores del administrador • Pérdida de equipos • Indisponibilidad del personal • Robo de equipos
Instalación	Daño muy grave a la organización	10	• Fuego • Daños por agua • Desastres naturales • Desastres industriales • Contaminación electromagnética • Corte del suministro eléctrico • Condiciones inadecuadas de temperatura o humedad • Pérdida de equipos • Robo de equipos
Servicios	Daño importante a la organización	6	• Fuego • Daños por agua • Desastres naturales • Desastres industriales • Contaminación electromagnética • Avería de origen físico o lógico • Corte del suministro eléctrico • Condiciones inadecuadas de temperatura o humedad • Fallo de servicios de comunicaciones • Degradación de los soportes de almacenamiento de la información • Errores de los usuarios • Errores del administrador • Errores de configuración • Difusión de software dañino • Errores de mantenimiento / actualización de programas (software) • Errores de mantenimiento / actualización de equipos (hardware)

			• Caída del sistema por agotamiento de recursos • Pérdida de equipos • Manipulación de la configuración • Abuso de privilegios de acceso • Denegación de servicio
Personal	Daño grave a la organización	7	• Fuego • Desastres naturales • Desastres industriales • Contaminación electromagnética • Pérdida de equipos • Indisponibilidad del personal • Suplantación de la identidad del usuario • Abuso de privilegios de acceso • Acceso no autorizado • Extorsión • Ingeniería social (picaresca)

Fuente: Autor

9.1.3 Valoración del riesgo para cada uno de los activos. A continuación se presenta una matriz de la valoración del riesgo según cada activo informático del Hospital San Francisco de Gachetá y en él se analiza en cada activo su clasificación, la clasificación del riesgo, la manera como se presenta, la valoración del riesgo y dentro de él probabilidad, impacto y riesgo determinando una aplicación de controles y el riesgo residual.

Para entender la matriz se deben tener en cuenta las siguientes tablas:

Tabla 11. Estimación de probabilidad

TABLA PARA ESTIMAR LA PROBABILIDAD	
VALOR	**DESCRIPCIÓN**
Muy bajo (1)	La amenaza se materializa a lo sumo una vez cada año.
Bajo (2)	La amenaza se materializa a lo sumo una vez cada semestre.
Medio (3)	La amenaza se materializa a lo sumo una vez cada mes.
Alto (4)	La amenaza se materializa a lo sumo una vez cada semana.
Muy alto (5)	La amenaza se materializa a lo sumo una vez cada día.

Fuente: Autor

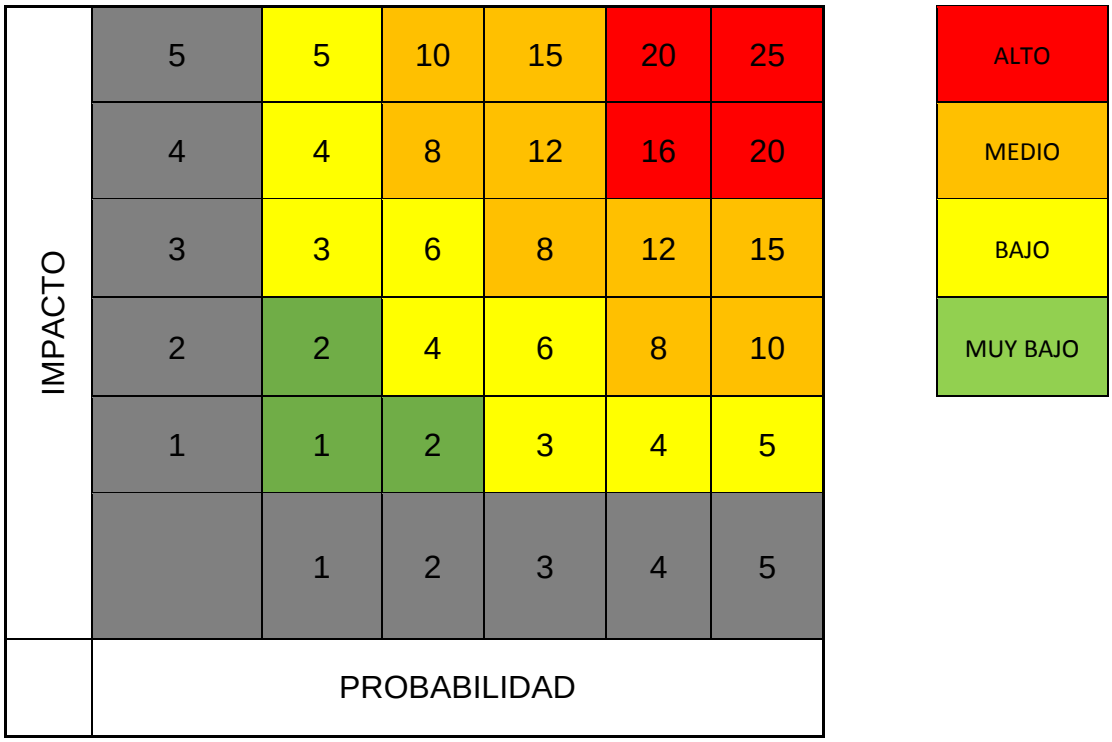
Tabla 12. Estimación del impacto

TABLA PARA ESTIMAR EL IMPACTO	
VALOR	**DESCRIPCIÓN**
Muy bajo (1)	El daño derivado de la materialización de la amenaza no tiene consecuencias muy relevantes para la organización.
Bajo (2)	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
Medio (3)	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
Alto (4)	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.
Muy alto (5)	El daño derivado de la materialización de la amenaza tiene consecuencias muy graves reseñables para la organización.

Fuente: Autor

Para determinar la valoración del riesgo en cada uno de los activos se debe tener en cuenta la tabla de valoración del riesgo mostrada a continuación la cual ha sido elaborada teniendo en cuenta las 4 dimensiones de valoración del riesgo establecidas por MAGERIT.

Tabla 13. Guía de valoración del riesgo



Fuente: Autor.

Una vez analizadas las vulnerabilidades se establece la valoración del riesgo, esto permitirá definir la aplicación de controles ISO 27001 – 27002 los cuales tendrán un nivel de eficacia según la tabla que se muestra a continuación:

Tabla 14. Eficacia del control

Eficacia de Control	
Alto	4
Medio	3
Bajo	2
Inexistente	1

Fuente: Autor.

Tras la implementación de controles y aplicación de los mismos se genera una mitigación del riesgo, lo anterior significa que el riesgo no ha sido erradicado por completo por lo que se genera una valoración de riesgo residual el cual el Hospital San Francisco de Gachetá asumirá según la siguiente tabla:

Tabla 15. Valoración del riesgo residual

VALORACIÓN DEL RIESGO RESIDUAL	
NIVEL DEL RIESGO RESIDUAL	**CALIFICACIÓN**
INACEPTABLE	> 16
IMPORTANTE	11 a 15
MODERADO	6 a 10
TOLERABLE	2 a 5
ACEPTABLE	< 2

Fuente: Autor.

Teniendo en cuenta lo anterior a continuación se relaciona la matriz de valoración del riesgo por activo informático del Hospital San Francisco de Gachetá.

Para calcular o estimar el valor o calificación del riesgo residual tendremos la siguiente formula:

$$\text{Riesgo residual} = \frac{\text{Valor del riesgo inherente}}{\text{Valor eficacia del control}}$$

El anterior resultado estará acompañado de un color según la tabla de la valoración del riesgo residual.

Tabla 16. Valoración del riesgo par activo informático.

RIESGO POR ACTIVO INFORMATICO HOSPITAL SAN FRANCISCO DE GACHETÁ																		
Activo/Amenaza	**Frecuencia**	**Valoración impacto potencial**					**Valoración riesgo potencial**					**Controles ISO 27001-27002**	**Eficacia de control**	**Valoración riesgo residual**				
		D	**I**	**C**	**A**	**T**	**D**	**I**	**C**	**A**	**T**			**D**	**I**	**C**	**A**	**T**
Bases de datos de CNT módulo de pacientes / ACTIVO DE INFORMACION																		
[N.*] Desastres naturales	1	3	3				3	3				11.1.4 Protección contra las amenazas externas y ambientales.	3	1,0	1,0			
[I.1] Fuego	1	3	3				3	3				11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5			
[I.2] Daños por agua	1	3	3				3	3				11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5			
[I.*] Desastres industriales	1	3	3				3	3				16.1.2 Notificación de los eventos de seguridad de la información.	2	1,5	1,5			
[I.4] Contaminación electromagnética	1	5	4				5	4				11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3			
[I.6] Corte del suministro eléctrico	4	5	4			4	20	16			16	12.6.1 Gestión de las vulnerabilidades técnicas.	4	5,0	4,0			4,0
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0		3,0

[E.2] Errores del administrador	3	4	4			3	12	12			9	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0			2,3
[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3		1,0
[E.16] Introducción de falsa información	2	4	4	5	5	3	8	8	10	10	6	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	1	4	5			5	4	5			5	12.3.1 Copias de seguridad de la información.	3	1,3	1,7			1,7
[E.19] Divulgación de información	3		4	5		3		12	15		9	13.2.4 Acuerdos de confidencialidad y secreto.	3		4,0	5,0		3,0
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0			1,5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	4	4			3	8	8			6	14.2.2 Procedimientos de control de cambios en los sistemas.	4	2,0	2,0			1,5
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0
[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5	8.1.1 Inventario de activos.	4	1,3	1,3	1,3		1,3
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6	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	3	3	3	3	3	2	9	9	9	9	6	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	2	4	5			4	8	10			8	12.2.1 Controles contra el código malicioso.	4	2,0	2,5			2,0
[A.11] Acceso no autorizado	2		5	5	5			10	10	10		9.1.1 Política de control de accesos.	4		2,5	2,5	2,5	

[A.15] Modificación de información	3	4	4	5	5	4	12	12	15	15	12	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	2	4	4	5	5	3	8	8	10	10	6	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	2		5	5	3	3		10	10	6	6	8.2.2 Etiquetado y manipulado de la información.	3		3,3	3,3	2,0	2,0
[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0		1,0
[A.19] Divulgación de información	4		4	5		3		16	20		12	13.2.4 Acuerdos de confidencialidad y secreto.	4		4,0	5,0		3,0
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0		1,0
[A.26] Ataque destructivo	1	5	5				5	5				12.3.1 Copias de seguridad de la información.	4	1,3	1,3			
Bases de datos financieras de CNT modulo tesorería, facturación y contable/ACTIVO DE INFORMACION																		
[N.*] Desastres naturales	1	3	3				3	3				11.1.4 Protección contra las amenazas externas y ambientales.	3	1,0	1,0			
[I.1] Fuego	1	3	3				3	3				11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5			
[I.2] Daños por agua	1	3	3				3	3				11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5			
[I.*] Desastres industriales	1	3	3				3	3				16.1.2 Notificación de los eventos de seguridad de la información.	2	1,5	1,5			
[I.4] Contaminación electromagnética	1	5	4				5	4				11.1.4 Protección contra las amenazas externas y	3	1,7	1,3			

												ambientales.						
[I.6] Corte del suministro eléctrico	4	5	4			4	20	16			16	12.6.1 Gestión de las vulnerabilidades técnicas.	4	5,0	4,0			4,0
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0		3,0
[E.2] Errores del administrador	3	4	4			3	12	12			9	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0			2,3
[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3		1,0
[E.16] Introducción de falsa información	2	4	4	5	5	3	8	8	10	10	6	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	1	4	5			5	4	5			5	12.3.1 Copias de seguridad de la información.	3	1,3	1,7			1,7
[E.19] Divulgación de información	3		4	5		3		12	15		9	13.2.4 Acuerdos de confidencialidad y secreto.	3		4,0	5,0		3,0
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0			1,5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	4	4			3	8	8			6	14.2.2 Procedimientos de control de cambios en los sistemas.	4	2,0	2,0			1,5
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0
[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5	8.1.1 Inventario de activos.	4	1,3	1,3	1,3		1,3

[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6	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	3	3	3	3	3	2	9	9	9	9	6	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	2	4	5			4	8	10			8	12.2.1 Controles contra el código malicioso.	4	2,0	2,5			2,0
[A.11] Acceso no autorizado	2		5	5	5			10	10	10		9.1.1 Política de control de accesos.	4		2,5	2,5	2,5	
[A.15] Modificación de información	3	4	4	5	5	4	12	12	15	15	12	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	2	4	4	5	5	3	8	8	10	10	6	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	2		5	5	3	3		10	10	6	6	8.2.2 Etiquetado y manipulado de la información.	3		3,3	3,3	2,0	2,0
[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0		1,0
[A.19] Divulgación de información	4		4	5		3		16	20		12	13.2.4 Acuerdos de confidencialidad y secreto.	4		4,0	5,0		3,0
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0		1,0
[A.26] Ataque destructivo	1	5	5				5	5				12.3.1 Copias de seguridad de la información.	4	1,3	1,3			
Bases de datos y documentos administrativos. CNT inventarios //ACTIVO DE INFORMACION																		
[N.*] Desastres naturales	1	3	3				3	3				11.1.4 Protección contra las amenazas externas y ambientales.	3	1,0	1,0			
[I.1] Fuego	1	3	3				3	3				11.1.4 Protección contra las amenazas externas y	2	1,5	1,5			

												ambientales.						
[I.2] Daños por agua	1	3	3			2	3	3			2	11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5			1,0
[I.*] Desastres industriales	1	3	3			2	3	3			2	11.1.4 Protección contra las amenazas externas y ambientales.	2	1,5	1,5			1,0
[I.4] Contaminación electromagnética	1	2	2			1	2	2			1	11.1.4 Protección contra las amenazas externas y ambientales.	3	0,7	0,7			0,3
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0			3,0
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[E.1] Errores de los usuarios	1	4	4	4		3	4	4	4		3	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	1,3	1,3	1,3		1,0
[E.2] Errores del administrador	1	4	4			3	4	4			3	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	1,0	1,0			0,8
[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3		1,0
[E.16] Introducción de falsa información	1	4	4	5	5	3	4	4	5	5	3	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	1	4	5			5	4	5			5	12.3.1 Copias de seguridad de la información.	3	1,3	1,7			1,7
[E.19] Divulgación de información	2		4	5		3		8	10		6	13.2.4 Acuerdos de confidencialidad y secreto.	3		2,7	3,3		2,0
[E.21] Errores de mantenimiento / actualización de programas (software)	1	4	4			3	4	4			3	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	1,0	1,0			0,8

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	5	4			4	5	4			4	14.2.2 Procedimientos de control de cambios en los sistemas.	4	1,3	1,0			1,0
[E.24] Caída del sistema por agotamiento de recursos	1	3	3			3	3	3			3	11.2.4 Mantenimiento de los equipos.	3	1,0	1,0			1,0
[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5	8.1.1 Inventario de activos.	4	1,3	1,3	1,3		1,3
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	2	4	5			4	8	10			8	12.2.1 Controles contra el código malicioso.	4	2,0	2,5			2,0
[A.11] Acceso no autorizado	2		5	5	5			10	10	10		9.1.1 Política de control de accesos.	4		2,5	2,5	2,5	
[A.14] Interceptación de información (escucha)	2		5	5	5	4		10	10	10	8	9.2.4 Gestión de información confidencial de autenticación de usuarios.	3		3,3	3,3	3,3	2,7
[A.15] Modificación de información	2	4	4	5	5	4	8	8	10	10	8	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	2	4	4	5	5	3	8	8	10	10	6	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	2		5	5	3	3		10	10	6	6	8.2.2 Etiquetado y manipulado de la información.	3		3,3	3,3	2,0	2,0
[A.18] Destrucción de la información	2	5	5	4		4	10	10	8		8	12.3.1 Copias de seguridad de la información.	4	2,5	2,5	2,0		2,0
[A.19] Divulgación de información	3		4	5				12	15			13.2.4 Acuerdos de confidencialidad y secreto.	4		3,0	3,8		
[A.25] Robo de equipos	2	4	4	4		4	8	8	8		8	11.1.3 Seguridad de oficinas, despachos y recursos.	4	2,0	2,0	2,0		2,0

[A.26] Ataque destructivo	2	5	5				10	10				12.3.1 Copias de seguridad de la información.	4	2,5	2,5			
Microsoft Windows 7 Professional/SOFTWARE																		
[I.4] Contaminación electromagnética	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0			3,0
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0		3,0
[E.2] Errores del administrador	3	4	4			3	12	12			9	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0			2,3
[E.4] Errores de configuración	2	4	4		4	4	8	8		8	8	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0		2,0	2,0
[E.8] Difusión de software dañino	2	4	5			4	8	10			8	12.2.1 Controles contra el código malicioso.	4	2,0	2,5			2,0
[E.20] Vulnerabilidades de los programas (software)	2	4	4		4	4	8	8		8	8	14.2.9 Pruebas de aceptación.	3	2,7	2,7		2,7	2,7
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0			1,5
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0

[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9	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	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	3	4	5			4	12	15			12	12.2.1 Controles contra el código malicioso.	4	3,0	3,8			3,0
[A.11] Acceso no autorizado	2		4	4	4			8	8	8		9.1.1 Política de control de accesos.	4		2,0	2,0	2,0	
[A.13] Repudio	2	4				3	8				6	9.1.2 Control de acceso a las redes y servicios asociados.	3	2,7				2,0
[A.22] Manipulación de programas	3	3	4	3	4	3	9	12	9	12	9	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	1	4	4			3	4	4			3	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0			0,8
[A.28] Indisponibilidad del personal	3	3				4	9				12	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	4,5				6
Windows server/SOFTWARE																		
[I.4] Contaminación electromagnética	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0

[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0			3,0
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0		3,0
[E.2] Errores del administrador	3	4	4			3	12	12			9	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0			2,3
[E.4] Errores de configuración	2	4	3			3	8	6			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5			1,5
[E.8] Difusión de software dañino	2	4	4				8	8				12.2.1 Controles contra el código malicioso.	4	2,0	2,0			
[E.20] Vulnerabilidades de los programas (software)	2	4	5	5		3	8	10	10		6	14.2.9 Pruebas de aceptación.	3	2,7	3,3	3,3		2,0
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0			1,5
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9	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	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	3	4	5			4	12	15			12	12.2.1 Controles contra el código malicioso.	4	3,0	3,8			3,0
[A.11] Acceso no autorizado	2		4	4	4			8	8	8		9.1.1 Política de control de accesos.	4		2,0	2,0	2,0	
[A.13] Repudio	2	5				4	10				8	9.1.2 Control de acceso a las redes y servicios asociados.	3	3,3				2,7
[A.22] Manipulación de programas	3	3	4	3	4	3	9	12	9	12	9	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	1	4	4			3	4	4			3	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0			0,8
[A.28] Indisponibilidad del personal	4	3				4	12				16	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	6				8
CNT programa de gestión administrativa, (programa eje del funcionamiento del hospital)/SOFTWARE																		
[I.4] Contaminación electromagnética	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0			3,0
[I.11] Emanaciones electromagnéticas	1	2	2			1	2	2			1	11.1.4 Protección contra las amenazas externas y ambientales.	3	0,7	0,7			0,3
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0		3,0

[E.2] Errores del administrador	3	4	4			3	12	12			9	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0			2,3
[E.4] Errores de configuración	2	4	3			3	8	6			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5			1,5
[E.8] Difusión de software dañino	2	4	4				8	8				12.2.1 Controles contra el código malicioso.	4	2,0	2,0			
[E.20] Vulnerabilidades de los programas (software)	2	4	5	5		3	8	10	10		6	14.2.9 Pruebas de aceptación.	3	2,7	3,3	3,3		2,0
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0			1,5
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9	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	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	3	4	5			4	12	15			12	12.2.1 Controles contra el código malicioso.	4	3,0	3,8			3,0
[A.11] Acceso no autorizado	2		5	5	5	2		10	10	10	4	9.1.1 Política de control de accesos.	4		2,5	2,5	2,5	1,0

[A.13] Repudio	2	5				5	10				10	9.1.2 Control de acceso a las redes y servicios asociados.	3	3,3				3,3
[A.22] Manipulación de programas	3	5	5	5	4	3	15	15	15	12	9	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	1	5	4			3	5	4			3	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,3	1,0			0,8
[A.28] Indisponibilidad del personal	4	4				4	16				16	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	8				8
CNT MODULO PACIENTES./SOFWARE																		
[I.4] Contaminación electromagnética	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0			3,0
[I.11] Emanaciones electromagnéticas	1	2	2			1	2	2			1	11.1.4 Protección contra las amenazas externas y ambientales.	3	0,7	0,7			0,3
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0		3,0
[E.2] Errores del administrador	3	4	4			3	12	12			9	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0			2,3
[E.4] Errores de configuración	2	4	3			3	8	6			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5			1,5

[E.8] Difusión de software dañino	2	4	4				8	8				12.2.1 Controles contra el código malicioso.	4	2,0	2,0			
[E.20] Vulnerabilidades de los programas (software)	2	4	5	5		3	8	10	10		6	14.2.9 Pruebas de aceptación.	3	2,7	3,3	3,3		2,0
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0			1,5
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9	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	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	3	4	5			4	12	15			12	12.2.1 Controles contra el código malicioso.	4	3,0	3,8			3,0
[A.11] Acceso no autorizado	2		5	5	5	2		10	10	10	4	9.1.1 Política de control de accesos.	4		2,5	2,5	2,5	1,0
[A.13] Repudio	2	5				5	10				10	9.1.2 Control de acceso a las redes y servicios asociados.	3	3,3				3,3
[A.22] Manipulación de programas	3	5	5	5	4	3	15	15	15	12	9	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	1	5	4			3	5	4			3	13.1.2 Mecanismos de seguridad asociados a	4	1,3	1,0			0,8

												servicios en red.						
[A.28] Indisponibilidad del personal	4	4				4	16				16	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	8				8
SISGEHOS./SOFWARE																		
[I.4] Contaminación electromagnética	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0			3,0
[I.11] Emanaciones electromagnéticas	1	2	2			1	2	2			1	11.1.4 Protección contra las amenazas externas y ambientales.	3	0,7	0,7			0,3
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0		3,0
[E.2] Errores del administrador	3	4	4			3	12	12			9	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0			2,3
[E.4] Errores de configuración	2	4	3			3	8	6			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5			1,5
[E.8] Difusión de software dañino	2	4	4				8	8				12.2.1 Controles contra el código malicioso.	4	2,0	2,0			
[E.20] Vulnerabilidades de los programas (software)	2	4	5	5		3	8	10	10		6	14.2.9 Pruebas de aceptación.	3	2,7	3,3	3,3		2,0
[E.21] Errores de mantenimiento / actualización de	2	4	4			3	8	8			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0			1,5

programas (software)																	
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9	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	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	3	4	5			4	12	15			12	12.2.1 Controles contra el código malicioso.	4	3,0	3,8			3,0
[A.11] Acceso no autorizado	2		5	5	5	2		10	10	10	4	9.1.1 Política de control de accesos.	4		2,5	2,5	2,5	1,0
[A.13] Repudio	2	5				5	10				10	9.1.2 Control de acceso a las redes y servicios asociados.	3	3,3				3,3
[A.22] Manipulación de programas	3	5	5	5	4	3	15	15	15	12	9	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	1	5	4			3	5	4			3	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,3	1,0			0,8
[A.28] Indisponibilidad del personal	4	4				4	16				16	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	8				8
GOOGLE CROME /SOFTWARE																		

[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0			3,0
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	4,0	4,0	4,0		3,0
[E.2] Errores del administrador	3	4	4			3	12	12			9	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0			2,3
[E.4] Errores de configuración	2	4	3			3	8	6			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5			1,5
[E.8] Difusión de software dañino	2	4	4				8	8				12.2.1 Controles contra el código malicioso.	4	2,0	2,0			
[E.20] Vulnerabilidades de los programas (software)	2	4	5	5		3	8	10	10		6	14.2.9 Pruebas de aceptación.	3	2,7	3,3	3,3		2,0
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0			1,5
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9	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	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	3	4	5			4	12	15			12	12.2.1 Controles contra el código malicioso.	4	3,0	3,8			3,0
[A.11] Acceso no autorizado	2		3	3	3			6	6	6		9.1.1 Política de control de accesos.	4		1,5	1,5	1,5	
[A.13] Repudio	2	3				3	6				6	9.1.2 Control de acceso a las redes y servicios asociados.	3	2,0				2,0
[A.24] Denegación de servicio	1	3	3			3	3	3			3	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	0,8	0,8			0,8
[A.28] Indisponibilidad del personal	3	4				4	12				12	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	12,0				12,0
[A.13] Repudio	2	2				2	4				4	9.1.2 Control de acceso a las redes y servicios asociados.	3	1,3				1,3
[A.22] Manipulación de programas	3	3	4	3	4	3	9	12	9	12	9	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	1	4	4			3	4	4			3	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0			0,8
[A.28] Indisponibilidad del personal	2	4				4	8				8	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	4				4
MOZILLA FIREFOX /SOFTWARE																		
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[I.6] Corte del suministro eléctrico	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	4	3,8	3,0			3,0
[E.1] Errores de los usuarios	3	4	4	4		3	12	12	12		9	7.2.2 Concienciación, educación y capacitación en	3	4,0	4,0	4,0		3,0

												seguridad de la información						
[E.2] Errores del administrador	3	4	4			3	12	12			9	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	3,0	3,0			2,3
[E.4] Errores de configuración	2	4	3			3	8	6			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5			1,5
[E.8] Difusión de software dañino	2	4	4				8	8				12.2.1 Controles contra el código malicioso.	4	2,0	2,0			
[E.20] Vulnerabilidades de los programas (software)	2	4	5	5		3	8	10	10		6	14.2.9 Pruebas de aceptación.	3	2,7	3,3	3,3		2,0
[E.21] Errores de mantenimiento / actualización de programas (software)	2	4	4			3	8	8			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	2,0			1,5
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9	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	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	3	4	5			4	12	15			12	12.2.1 Controles contra el código malicioso.	4	3,0	3,8			3,0
[A.11] Acceso no autorizado	2		3	3	3			6	6	6		9.1.1 Política de control de accesos.	4		1,5	1,5	1,5	
[A.13] Repudio	2	3				3	6				6	9.1.2 Control de acceso a las redes y servicios asociados.	3	2,0				2,0
[A.24] Denegación de servicio	1	3	3			3	3	3			3	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	0,8	0,8			0,8
[A.28] Indisponibilidad del personal	3	4				4	12				12	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	12,0				12,0
[A.13] Repudio	2	2				2	4				4	9.1.2 Control de acceso a las redes y servicios asociados.	3	1,3				1,3
[A.22] Manipulación de programas	3	3	4	3	4	3	9	12	9	12	9	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	1	4	4			3	4	4			3	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0			0,8
[A.28] Indisponibilidad del personal	2	4				4	8				8	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	4				4
34 puestos de trabajo (COMPUTADORES)/HARDWARE																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y	3	1,3	1,3			1,3

												ambientales.						
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.3] Contaminación mecánica	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.4] Contaminación electromagnética	2	4	4			4	8	8			8	11.1.4 Protección contra las amenazas externas y ambientales.	3	2,7	2,7			2,7
[I.5] Avería de origen físico o lógico	3	4	4			4	12	12			12	11.2.4 Mantenimiento de los equipos.	4	3,0	3,0			3,0
[I.6] Corte del suministro eléctrico	4	5	4			4	20	16			16	12.6.1 Gestión de las vulnerabilidades técnicas.	4	5,0	4,0			4,0
[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	4			4	10	8			8	11.1.4 Protección contra las amenazas externas y ambientales.	3	3,3	2,7			2,7
[I.8] Fallo de servicios de comunicaciones	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	3	5,0	4,0			4,0
[I.9] Interrupción de otros servicios o suministros esenciales	2	5	4			4	10	8			8	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7			2,7
[I.11] Emanaciones electromagnéticas	2	4	4			4	8	8			8	11.1.4 Protección contra las amenazas externas y ambientales.	2	4,0	4,0			4,0
[E.24] Caída del sistema por agotamiento de	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0

recursos																		
[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5	8.1.1 Inventario de activos.	4	1,3	1,3	1,3		1,3
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9	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	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	2					4					8	8.1.3 Uso aceptable de los activos.	2					4,0
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0		1,0
[A.26] Ataque destructivo	2	5	5			3	10	10			6	12.3.1 Copias de seguridad de la información.	4	2,5	2,5			1,5
[A.27] Ocupación enemiga	1	5	5			4	5	5			4	11.1.2 Controles físicos de entrada.	4	1,3	1,3			1,0
[A.28] Indisponibilidad del personal	2	4				4	8				8	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	4				4
Servidor local/HARDWARE																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3

[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.3] Contaminación mecánica	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.4] Contaminación electromagnética	2	4	4			4	8	8			8	11.1.4 Protección contra las amenazas externas y ambientales.	3	2,7	2,7			2,7
[I.5] Avería de origen físico o lógico	3	4	4			4	12	12			12	11.2.4 Mantenimiento de los equipos.	4	3,0	3,0			3,0
[I.6] Corte del suministro eléctrico	4	5	4			4	20	16			16	12.6.1 Gestión de las vulnerabilidades técnicas.	4	5,0	4,0			4,0
[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	4			4	10	8			8	11.1.4 Protección contra las amenazas externas y ambientales.	3	3,3	2,7			2,7
[I.8] Fallo de servicios de comunicaciones	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	3	5,0	4,0			4,0
[I.9] Interrupción de otros servicios o suministros esenciales	2	5	4			4	10	8			8	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7			2,7
[I.11] Emanaciones electromagnéticas	2	4	4			4	8	8			8	11.1.4 Protección contra las amenazas externas y ambientales.	2	4,0	4,0			4,0

[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0
[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5	8.1.1 Inventario de activos.	4	1,3	1,3	1,3		1,3
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.4] Manipulación de la configuración	3	5	5	4	5	3	15	15	12	15	9	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	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	2					4					8	8.1.3 Uso aceptable de los activos.	2					4,0
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0		1,0
[A.26] Ataque destructivo	2	5	5			3	10	10			6	12.3.1 Copias de seguridad de la información.	4	2,5	2,5			1,5
[A.27] Ocupación enemiga	1	5	5			4	5	5			4	11.1.2 Controles físicos de entrada.	4	1,3	1,3			1,0
[A.28] Indisponibilidad del personal	2	4				4	8				8	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	8,0				8,0
Router/RED																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3

[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[I.6] Corte del suministro eléctrico	4	5	4			4	20	16			16	12.6.1 Gestión de las vulnerabilidades técnicas.	4	5,0	4,0			4,0
[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	4			4	10	8			8	11.1.4 Protección contra las amenazas externas y ambientales.	3	3,3	2,7			2,7
[E.1] Errores de los usuarios	2	4	4	4		3	8	8	8		6	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	2,7	2,7	2,7		2,0
[E.4] Errores de configuración	2	4	3			3	8	6			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5			1,5
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	2	5	4			4	10	8			8	14.2.2 Procedimientos de control de cambios en los sistemas.	4	2,5	2,0			2,0
[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5	8.1.1 Inventario de activos.	4	1,3	1,3	1,3		1,3
[A.4] Manipulación de la configuración	2	5	5	4	5	3	10	10	8	10	6	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	1	3	3	3	3	2	3	3	3	3	2	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	1	3	3	5	3		3	3	5	3		9.1.1 Política de control de accesos.	4	0,8	0,8	1,3	0,8	
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0		1,0
[A.26] Ataque destructivo	1	5	5			3	5	5			3	12.3.1 Copias de seguridad de la información.	4	1,3	1,3			0,8
[A.28] Indisponibilidad del personal	2	4				4	8				8	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	4				4
3 Swicth/RED																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0

[I.6] Corte del suministro eléctrico	4	5	4			4	20	16			16	12.6.1 Gestión de las vulnerabilidades técnicas.	4	5,0	4,0			4,0
[I.7] Condiciones inadecuadas de temperatura o humedad	2	5	4			4	10	8			8	11.1.4 Protección contra las amenazas externas y ambientales.	3	3,3	2,7			2,7
[E.4] Errores de configuración	1	4	3			3	4	3			3	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	1,0	0,8			0,8
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	1	5	4			4	5	4			4	14.2.2 Procedimientos de control de cambios en los sistemas.	4	1,3	1,0			1,0
[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5	8.1.1 Inventario de activos.	4	1,3	1,3	1,3		1,3
[A.4] Manipulación de la configuración	1	5	5	4	5	3	5	5	4	5	3	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	1	3	3	3	3	2	3	3	3	3	2	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	1	3	3	5	3		3	3	5	3		9.1.1 Política de control de accesos.	4	0,8	0,8	1,3	0,8	
[A.26] Ataque destructivo	1	5	5			3	5	5			3	12.3.1 Copias de seguridad de la información.	4	1,3	1,3			0,8
[A.28] Indisponibilidad del personal	1	4				4	4				4	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	2				2
Cableado estructurado/INSTALACION																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y	3	1,3	1,3			1,3

												ambientales.						
[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3			1,3
[E.1] Errores de los usuarios	1	4	4	4		3	4	4	4		3	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	1,3	1,3	1,3		1,0
[A.26] Ataque destructivo	1	5	5			3	5	5			3	12.3.1 Copias de seguridad de la información.	4	1,3	1,3			0,8
[A.28] Indisponibilidad del personal	1	4				4	4				4	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	2				2
Instalaciones eléctricas trifásicas no regulada /INSTALACION																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3

[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3			1,3
[E.1] Errores de los usuarios	1	4	4	4		3	4	4	4		3	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	1,3	1,3	1,3		1,0
[A.26] Ataque destructivo	1	5	5			3	5	5			3	12.3.1 Copias de seguridad de la información.	4	1,3	1,3			0,8
[A.28] Indisponibilidad del personal	1	4				4	4				4	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	2	2				2
Planta de energía eléctrica/EQUIPAMENTO AUXILIAR																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3

[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3			1,3
[E.1] Errores de los usuarios	1	4	4	4		3	4	4	4		3	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	1,3	1,3	1,3		1,0
[A.26] Ataque destructivo	1	5	5			3	5	5			3	12.3.1 Copias de seguridad de la información.	4	1,3	1,3			0,8
[A.28] Indisponibilidad del personal	1	4				4	4				4	7.2.2 Concienciación, educación y capacitación en seguridad de la información	2	2				2
Conectividad de Internet 2Mb/SERVICIOS																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0

[I.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.4] Contaminación electromagnética	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.5] Avería de origen físico o lógico	2	4	4			4	8	8			8	11.2.4 Mantenimiento de los equipos.	4	2,0	2,0			2,0
[I.6] Corte del suministro eléctrico	4	5	4			4	20	16			16	12.6.1 Gestión de las vulnerabilidades técnicas.	4	5,0	4,0			4,0
[I.8] Fallo de servicios de comunicaciones	2	5	4			4	10	8			8	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7			2,7
[E.1] Errores de los usuarios	2	4	4	4		3	8	8	8		6	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	2,7	2,7	2,7		2,0
[E.2] Errores del administrador	1	4	4			3	4	4			3	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	1,0	1,0			0,8
[E.4] Errores de configuración	2	4	3			3	8	6			6	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	2,0	1,5			1,5
[E.8] Difusión de software dañino	1	4	4				4	4				12.2.1 Controles contra el código malicioso.	4	1,0	1,0			
[E.24] Caída del sistema por agotamiento de recursos	3	3	3			3	9	9			9	11.2.4 Mantenimiento de los equipos.	3	3,0	3,0			3,0
[E.25] Pérdida de equipos	1	5	5	5		5	5	5	5		5	8.1.1 Inventario de activos.	4	1,3	1,3	1,3		1,3
[E.28] Indisponibilidad del personal	1	3	3			3	3	3			3	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	1,0	1,0			1,0

[A.4] Manipulación de la configuración	1	5	5	4	5	3	5	5	4	5	3	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	1	2	2			2	2	2			2	13.1.1 Controles de red.	4	0,5	0,5			0,5
[A.13] Repudio	1	4				3	4				3	9.2.4 Gestión de información confidencial de autenticación de usuarios.	3	1,3				1,0
[A.14] Interceptación de información (escucha)	1		4	4	4	4		4	4	4	4	9.2.4 Gestión de información confidencial de autenticación de usuarios.	3		1,3	1,3	1,3	1,3
[A.16] Introducción de falsa información	1	4	4	5	5	3	4	4	5	5	3	9.4.1 Restricción del acceso a la información.	4	1,0	1,0	1,3	1,3	0,8
[A.24] Denegación de servicio	1	4	4			3	4	4			3	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0			0,8
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0		1,0
[A.26] Ataque destructivo	1	5	5			3	5	5			3	12.3.1 Copias de seguridad de la información.	4	1,3	1,3			0,8
Servicio de mantenimiento infraestructura. /SERVICIOS																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y	2	2,0	2,0			2,0

												ambientales.						
[I.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.5] Avería de origen físico o lógico	1	4	4			4	4	4			4	11.2.4 Mantenimiento de los equipos.	4	1,0	1,0			1,0
[I.6] Corte del suministro eléctrico	4	5	4			4	20	16			16	12.6.1 Gestión de las vulnerabilidades técnicas.	4	5,0	4,0			4,0
[I.8] Fallo de servicios de comunicaciones	2	5	4			4	10	8			8	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7			2,7
[E.1] Errores de los usuarios	2	4	4	4		3	8	8	8		6	7.2.2 Concienciación, educación y capacitación en seguridad de la información	3	2,7	2,7	2,7		2,0
[E.2] Errores del administrador	2	4	4			3	8	8			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	4	2,0	2,0			1,5
[E.4] Errores de configuración	1	4	3			3	4	3			3	14.2.5 Uso de principios de ingeniería en protección de sistemas.	4	1,0	0,8			0,8
[E.8] Difusión de software dañino	1	4	4				4	4				12.2.1 Controles contra el código malicioso.	4	1,0	1,0			
[E.28] Indisponibilidad del personal	1	3	3			3	3	3			3	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	1,0	1,0			1,0
[A.4] Manipulación de la configuración	2	5	5	4	5	3	10	10	8	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	1		5	5	4	4		5	5	4	4	8.2.2 Etiquetado y manipulado de la información.	3		1,7	1,7	1,3	1,3
[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0		1,0
[A.19] Divulgación de información	2		4	5				8	10			13.2.4 Acuerdos de confidencialidad y secreto.	4		2,0	2,5		
[A.24] Denegación de servicio	1	4	4			3	4	4			3	13.1.2 Mecanismos de seguridad asociados a servicios en red.	4	1,0	1,0			0,8
[A.25] Robo de equipos	1	4	4	4		4	4	4	4		4	11.1.3 Seguridad de oficinas, despachos y recursos.	4	1,0	1,0	1,0		1,0
[A.26] Ataque destructivo	1	5	5			3	5	5			3	12.3.1 Copias de seguridad de la información.	4	1,3	1,3			0,8
Ingeniero de sistemas/PERSONAL																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3			1,3

[I.8] Fallo de servicios de comunicaciones	2	5	4			4	10	8			8	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7			2,7
[E.7] Deficiencias en la organización	2					4					8	6.1.1 Asignación de responsabilidades para la seguridad de la información.	4					2,0
[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3		1,0
[E.16] Introducción de falsa información	1	5	5	5		4	5	5	5		4	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3		1,0
[E.18] Destrucción de la información	1	4	5			5	4	5			5	12.3.1 Copias de seguridad de la información.	3	1,3	1,7			1,7
[E.19] Divulgación de información	2		4	5		3		8	10		6	13.2.4 Acuerdos de confidencialidad y secreto.	3		2,7	3,3		2,0
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	1		5	5	4	4		5	5	4	4	8.2.2 Etiquetado y manipulado de la información.	3		1,7	1,7	1,3	1,3
[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0		1,0
[A.19] Divulgación de información	2		4	5				8	10			13.2.4 Acuerdos de confidencialidad y secreto.	4		2,0	2,5		
[A.28] Indisponibilidad del personal	2	4				4	8				8	7.2.2 Concienciación, educación y capacitación en seguridad de la información	2	4				4

[A.30] Ingeniería social (picaresca)	2		5	5		4		10	10		8	7.2.2 Concienciación, educación y capacitación en seguridad de la información	4		2,5	2,5		2,0
Tecnólogo de sistemas/PERSONAL																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3			1,3
[I.8] Fallo de servicios de comunicaciones	2	5	4			4	10	8			8	12.6.1 Gestión de las vulnerabilidades técnicas.	3	3,3	2,7			2,7
[E.7] Deficiencias en la organización	2					4					8	6.1.1 Asignación de responsabilidades para la seguridad de la información.	4					2,0
[E.15] Alteración de la información	1	5	5	5		4	5	5	5		4	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3		1,0
[E.16] Introducción de falsa información	1	5	5	5		4	5	5	5		4	9.4.1 Restricción del acceso a la información.	4	1,3	1,3	1,3		1,0
[E.18] Destrucción de la información	1	4	5			5	4	5			5	12.3.1 Copias de seguridad de la información.	3	1,3	1,7			1,7

[E.19] Divulgación de información	2		4	5		3		8	10		6	13.2.4 Acuerdos de confidencialidad y secreto.	3		2,7	3,3		2,0
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	1		5	5	4	4		5	5	4	4	8.2.2 Etiquetado y manipulado de la información.	3		1,7	1,7	1,3	1,3
[A.18] Destrucción de la información	1	5	5	4		4	5	5	4		4	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0		1,0
[A.19] Divulgación de información	4		4	5				16	20			13.2.4 Acuerdos de confidencialidad y secreto.	4		4,0	5,0		
[A.28] Indisponibilidad del personal	2	4				4	8				8	7.2.2 Concienciación, educación y capacitación en seguridad de la información	2	4				4
[A.30] Ingeniería social (picaresca)	2		5	5		4		10	10		8	7.2.2 Concienciación, educación y capacitación en seguridad de la información	4		2,5	2,5		2,0
34 usuarios finales./PERSONAL																		
[N.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.2] Daños por agua	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,3	1,3			1,3
[N.*] Desastres naturales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y	3	1,3	1,3			1,3

												ambientales.						
[I.1] Fuego	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.*] Desastres industriales	1	4	4			4	4	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	2	2,0	2,0			2,0
[I.7] Condiciones inadecuadas de temperatura o humedad	1	5	4			4	5	4			4	11.1.4 Protección contra las amenazas externas y ambientales.	3	1,7	1,3			1,3
[I.8] Fallo de servicios de comunicaciones	3	5	4			4	15	12			12	12.6.1 Gestión de las vulnerabilidades técnicas.	3	5,0	4,0			4,0
[E.7] Deficiencias en la organización	2					4					8	6.1.1 Asignación de responsabilidades para la seguridad de la información.	4					2,0
[E.15] Alteración de la información	2	5	5	5		4	10	10	10		8	9.4.1 Restricción del acceso a la información.	4	2,5	2,5	2,5		2,0
[E.16] Introducción de falsa información	2	5	5	5		4	10	10	10		8	9.4.1 Restricción del acceso a la información.	4	2,5	2,5	2,5		2,0
[E.18] Destrucción de la información	1	4	5			5	4	5			5	12.3.1 Copias de seguridad de la información.	3	1,3	1,7			1,7
[E.19] Divulgación de información	2		5	5		3		10	10		6	13.2.4 Acuerdos de confidencialidad y secreto.	3		3,3	3,3		2,0
[E.28] Indisponibilidad del personal	2	3	3			3	6	6			6	7.2.2 Concienciación, educación y capacitación en seguridad de la información.	3	2,0	2,0			2,0
[A.5] Suplantación de la identidad del usuario	2	3	5	5	5	3	6	10	10	10	6	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	2	3	3	3	3	2	6	6	6	6	4	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	2		5	5	4	4		10	10	8	8	8.2.2 Etiquetado y manipulado de la información.	3		3,3	3,3	2,7	2,7
[A.18] Destrucción de la información	1	5	5	4		5	5	5	4		5	12.3.1 Copias de seguridad de la información.	4	1,3	1,3	1,0		1,3
[A.19] Divulgación de información	5		4	5				20	25			13.2.4 Acuerdos de confidencialidad y secreto.	4		5,0	6,3		
[A.28] Indisponibilidad del personal	4	4				4	16				16	7.2.2 Concienciación, educación y capacitación en seguridad de la información	2	8				8
[A.30] Ingeniería social (picaresca)	3		5	5		4		15	15		12	7.2.2 Concienciación, educación y capacitación en seguridad de la información	4		3,8	3,8		3,0

Fuente: Autor

9.2 CONTROLES ISO 27001 - 27002 A IMPLEMENTAR

Los controles ISO 27001 – 27002 permiten diseñar políticas que mitiguen la materialización de amenazas para los activos de información, de acuerdo a estos controles se pueden establecer parámetros que determinan la posibilidad de aceptación o el nivel de un riesgo residual para el cual se deben establecer acciones que mitiguen materialización de riesgos, para el caso particular del Hospital San Francisco de Gachetá se tienen en cuenta dominios que respondan a aspectos de dirección de seguridad de la información, asignación de responsabilidades, perfiles para contratación por parte del departamento de recursos humanos, gestión de los activos de información, controles de acceso a los activos de información, dominios que permitan establecer controles de seguridad ambiental y física, seguridad operativa, seguridad en telecomunicaciones y controles que garanticen el mantenimiento y puesta en marcha de los activos de información de la entidad hospitalaria.

Tras el análisis de riesgos por activos realizado anteriormente en la tabla 16 se presenta a continuación el resumen de los controles a implementar en el Hospital San Francisco de Gachetá teniendo en cuenta de manera global los dominios con sus respectivos objetivos y controles los cuales permiten ser la base de las políticas de seguridad informática expuestas en el capítulo 10 del presente documento y que están dirigidas a la mitigación del riesgo en los activos de información en la entidad hospitalaria.

Tabla 17. Controles ISO 27001 - 27002 a implementar.

DOMINIO	OBJETIVO - CONTROL
5. POLÍTICAS DE SEGURIDAD.	**5.1 Directrices de la Dirección en seguridad de la información** 5.1.1 Conjunto de políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.	**6.1 Organización interna.** 6.1.1 Asignación de responsabilidades para la seguridad de la información. 6.1.3 Contacto con las autoridades.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	**7.1 Antes de la contratación.** 7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación.
	7.2 Durante la contratación. 7.2.1Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en seguridad de la información. 7.2.3 Proceso disciplinario
8. GESTIÓN DE ACTIVOS.	**8.1 Responsabilidad sobre los activos** 8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos.
9. CONTROL DE ACCESOS.	**9.3Responsabilidades del usuario.** 9.3.1 Uso de información confidencial para la autenticación.
	9.4 Control de acceso a sistemas y aplicaciones. 9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario
11. SEGURIDAD FÍSICA Y AMBIENTAL.	**11.1 Áreas seguras.** 11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga.

	11.2 Seguridad de los equipos. 11.2.1 Emplazamiento y protección de equipos. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.
12. SEGURIDAD EN LA OPERATIVA.	**12.2 Protección contra código malicioso.** 12.2.1 Controles contra el código malicioso.
	12.3 Copias de seguridad. 12.3.1 Copias de seguridad de la información.
	12.4 Registro de actividad y supervisión. 12.4.1 Registro y gestión de eventos de actividad.
	12.5 Control del software en explotación. 12.5.1 Instalación del software en sistemas en producción.
	12.6 Gestión de la vulnerabilidad técnica. 12.6.1 Gestión de las vulnerabilidades técnicas 12.6.2 Restricciones en la instalación de software.
13. SEGURIDAD EN LAS TELECOMUNICACIONES.	**13.1 Gestión de la seguridad en las redes.** 13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes.
	13.2 Intercambio de información con partes externas. 13.2.4 Acuerdos de confidencialidad y secreto.
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.	**14.1 Requisitos de seguridad de los sistemas de información.** 14.1.1 Análisis y especificación de los requisitos de seguridad
	14.2 Seguridad en los procesos de desarrollo y soporte. 14.2.1 Política de desarrollo seguro de software

Fuente: autor

10. POLÍTICAS DE SEGURIDAD INFORMÁTICA PARA EL HOSPITAL SAN FRANCISCO DE GACHETÁ

Respondiendo a las necesidades de seguridad de información del Hospital San Francisco de Gachetá se hace necesario establecer una serie de procesos que respondan a los controles establecidos según la ISO 27001-27002, lo anterior permite mitigar amenazas que de ser materializadas pueden generar un colapso en el servicio hospitalario brindado desde el área administrativa y de historias clínicas del hospital San Francisco de Gachetá. Los procesos que responden a este tipo de necesidades de mitigación del riesgo han sido determinados bajo el marco de políticas de seguridad informática, las cuales son el resultado del análisis de riesgos activo por activo, teniendo en cuenta la clasificación de cada uno y respondiendo a los diferentes controles de la ISO 27001 – 27002.

De acuerdo a lo anterior, se relacionan las siguientes políticas de seguridad establecidas:

Tabla 18 Políticas de seguridad de la información.

Política	1. **Políticas de seguridad de la información.**
Objetivo	Asegurar los activos de la información a través de la implementación de controles de seguridad que permitan garantizar la integridad y disponibilidad de los activos de información.
Aplicabilidad	Dirigida a todos los funcionarios y equipos del Hospital San Francisco de Gachetá del área administrativa y de historias clínicas que utilice para el ejercicio de sus funciones activos informáticos en sus diferentes clasificaciones y que contengan información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	
✓ El Hospital San Francisco de Gachetá mantendrá un inventario de sus activos informáticos ✓ El departamento de sistemas del Hospital San Francisco de Gachetá tendrá un inventario actualizado del software instalado en los equipos de cómputo y prohibirá la instalación de programas ajenos al inventario institucional.	

✓ Todo Software debe responder a una necesidad para su instalación, y debe responder a una licencia de su autor inventariada según cada equipo de cómputo. Analizar, diseñar e implementar programas de auditoria interna para el sistema de gestión de seguridad informática en los activos de información del área administrativa y de historias clínicas del hospital.

✓ Todo el personal debe contener una contraseña asignada por el departamento de sistemas y esta debe responder a un alto nivel de seguridad, la adjudicación de esta contraseña es responsabilidad del departamento de sistemas y es responsabilidad del empleado mantenerla en secreto y no transferirla a terceros.

✓ El departamento de sistemas realizara una revisión periódica según cronograma para verificar descargas o instalaciones no autorizadas de programas en los equipos del Hospital.

✓ Los empleados no podrán utilizar los activos de información para fines personales.

✓ Los empleados no podrán utilizar los activos de información para ingresar a servicios de internet diferentes a los requeridos para el cumplimiento de sus funciones.

✓ Los empleados no deberán utilizar medios de almacenamiento externos diferentes a los que son propiedad del Hospital.

✓ Están prohibidas las copias de correos, bases de datos, archivos administrativos sin previa autorización y la exportación de estos a medios de almacenamiento diferentes a los del Hospital San Francisco de Gachetá.

✓ Es responsabilidad de los empleados conocer el funcionamiento de equipos como escáner, impresoras entre otros, en caso de no conocer debe solicitar instrucción al departamento de sistemas del Hospital.

✓ Está completamente prohibida la manipulación, desensamble, adaptación o modificación de los equipos de cómputo por parte de empleados, esta función es del departamento de sistemas.

Responsables	Departamento de sistemas, funcionarios del área administrativa y de historias clínicas, gerencia y recursos humanos
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Autor

Tabla 19. Políticas de capacitación y concientización de seguridad de la información.

Política	**2. Políticas de capacitación y concientización de seguridad de la información.**
Objetivo	Mitigar la indisponibilidad del personal ante incidentes de seguridad de la información a través de procesos de capacitación y concientización dirigidos a los funcionarios del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá.
Aplicabilidad	Dirigida a todos los funcionarios y equipos del Hospital San Francisco de Gachetá del área administrativa y de historias clínicas que utilice para el ejercicio de sus funciones activos informáticos en sus diferentes clasificaciones y que contengan información relevante que representen riesgo para el correcto modelo operacional de la entidad de salud tanto en su administración como en la atención oportuna de sus pacientes.
Directrices específicas:	

✓ El Hospital San Francisco de Gachetá identificará acciones o procedimientos realizados de manera incorrecta con el fin de generar un proceso de capacitación para mejora de procesos

✓ El departamento de sistemas del Hospital San Francisco de Gachetá identificará acciones o procedimientos realizados por los funcionarios del área administrativa y de historias clínicas que representen riesgo para los activos de información.

✓ La gerencia del Hospital San Francisco de Gachetá generará convocatorias para licitar contratos de capacitación en seguridad informática con expertos las cuales estarán dirigidas a los funcionarios del área administrativa y de historias clínicas del hospital San Francisco de Gachetá.

✓ Una vez detectadas las fallas en seguridad por parte del departamento de sistemas gerencia dispone de un mes de plazo para licitar y generar los planes de capacitación.

✓ Los funcionarios deben asistir a la capacitación y es obligación cumplir con la totalidad de las horas establecidas para tal fin.

✓ La empresa externa o personal externo que realice la capacitación debe

certificar a los funcionarios sobre el cumplimiento y aprobación de la misma.	
Responsables	Departamento de sistemas, funcionarios del área administrativa y de historias clínicas, gerencia y recursos humanos.
Sanciones	Suspensión temporal del cargo, retiro del cargo.

Fuente: Autor

Tabla 20. Políticas de confidencialidad

Política	**3. Políticas de confidencialidad**
Objetivo	Evitar de manera efectiva la divulgación de la información estableciendo controles y acuerdos de confidencialidad con los funcionarios del área administrativa y de historias clínicas del hospital San Francisco de Gachetá.
Aplicabilidad	Dirigida a los funcionarios del departamento de sistemas, gerencia, recursos humanos, y de historias clínicas del Hospital San Francisco de Gachetá.
Directrices específicas:	
✓ La gerencia del Hospital San Francisco de Gachetá emitirá una circular informativa sobre los perjuicios que representa para la entidad la divulgación de la información dirigida a sus funcionarios en general. ✓ La gerencia y el departamento de talento humano realizarán una reunión informativa dirigida a los funcionarios del área administrativa y de historias clínicas con el fin de notificarles las sanciones legales y laborales a las que habrá lugar en caso de incumplir el acuerdo de confidencialidad, esto se realizará previo a la firma por parte de los funcionarios del acuerdo de confidencialidad. ✓ Talento humano emitirá un acuerdo de confidencialidad dirigido a los funcionarios en general la cual debe ser firmada con copia a la hoja de vida donde se establecen los procesos y procedimientos que se deben ejecutar para evitar la divulgación de la información.	
Responsables	Funcionarios de oficinas administrativas, funcionarios de historias clínicas, recursos humanos, departamento de sistemas, dirección general.
Sanciones	Suspensión temporal del cargo, retiro del cargo.

Fuente: Autor

Tabla 21. Políticas de fluido eléctrico.

Política	**4. Políticas de fluido eléctrico.**
Objetivo	Garantizar el constante suministro eléctrico en las instalaciones del Hospital San Francisco de Gachetá mitigando la interrupción del servicio por cortes eléctricos.
Aplicabilidad	Dirigida a los funcionarios del departamento de sistemas, funcionarios de infraestructura.
Directrices específicas:	
✓ La gerencia del Hospital San Francisco de Gachetá solicitara a la empresa de energía de Cundinamarca se informe con antelación sobre cortes programados en el servicio eléctrico con el fin de asumir las acciones pertinentes. ✓ El departamento de infraestructura verificará el estado actual de la planta eléctrica y realizará mantenimientos preventivos y correctivos los cuales responderán a un cronograma anual de trabajo de acuerdo a las indicaciones del fabricante, dicho mantenimiento se podrá realizar por los funcionarios capacitados del departamento de infraestructura, en caso de declararse impedidos se debe solicitar a la gerencia la contratación de personal externo para la ejecución del mantenimiento. ✓ El departamento de sistemas analizará la necesidad de instalación de UPS en el área administrativa y de historias clínicas, de acuerdo a dicha necesidad se creará el plan de compras para adquirir los equipos necesarios con el fin de garantizar el constante fluido eléctrico. ✓ Es responsabilidad de la gerencia facilitar los recursos financieros y técnicos a los departamentos de sistemas y de infraestructura con el fin de responder al cronograma de mantenimiento preventivo y correctivo del equipamiento auxiliar.	
Responsables	Departamento de sistemas, Dirección general y departamento de infraestructura.
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo.

Fuente: Autor

Tabla 22. Políticas de aspectos organizativos de la seguridad de la información.

Política	**5. Políticas de aspectos organizativos de la seguridad de la información.**
Objetivo	Establecer responsabilidades según la asignación de funciones para mejorar el nivel de seguridad informática en el área

	administrativa y de historias clínicas del Hospital San Francisco de Gachetá.
Aplicabilidad	Dirigida a los funcionarios del departamento de sistemas, gerencia, recursos humanos, y de historias clínicas del Hospital San Francisco de Gachetá.
Directrices específicas:	
✓ Las funciones de cada uno de los funcionarios debe estar en el manual de procedimientos. ✓ Cada funcionario tendrá asignada una contraseña para acceso a los activos de información, su asignación es responsabilidad del departamento de sistemas del hospital. ✓ Los funcionarios deben permanecer dentro de sus dependencias en los horarios establecidos, a excepción de aquellos a quienes les sea otorgado un permiso o se haya cambiado el horario por notificación escrita (físico o digital) de su jefe inmediato con respectiva copia a la oficina de recursos humanos. ✓ Es responsabilidad de los funcionarios conocer el correcto funcionamiento de los activos informáticos. ✓ Es responsabilidad del departamento de sistemas capacitar a los funcionarios con relación al correcto funcionamiento de los activos de información y realizar una constante evaluación del desempeño de los funcionarios generando un informe semestral al área de talento humano. ✓ Es responsabilidad de talento humano informar al departamento de sistemas sobre vinculación o desvinculación de los funcionarios para realizar los procesos de asignación de credenciales de acceso o eliminación de las mismas, en caso de desvinculación el departamento de sistemas generará un paz y salvo del exfuncionario dirigido a talento humano para proceder con liquidación u otros trámites pertinentes. ✓ Es responsabilidad de los funcionarios la custodia de sus credenciales de acceso, esta debe ser intransferible y de uso personal, en caso contrario se generar un reporte negativo con respectiva sanción disciplinaria por parte de recursos humanos.	
Responsables	Funcionarios de oficinas administrativas, funcionarios de historias clínicas, recursos humanos, departamento de sistemas.
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo.

Fuente: Autor

Tabla 23. Políticas de seguridad ligada a los recursos humanos.

Política	**6. Políticas de seguridad ligada a los recursos humanos.**
Objetivo	Establecer parámetros para garantizar una adecuada protección de los activos de información del Hospital San Francis de Gachetá desde el área de recursos humanos.
Aplicabilidad	Dirigida a los funcionarios del departamento de sistemas, gerencia, recursos humanos, del Hospital San Francisco de Gachetá.
Directrices específicas:	
✓ Se deben definir los perfiles de aspirantes a vacantes que respondan a los requerimientos para el correcto uso de los activos de información. ✓ Se deben verificar los antecedentes de los aspirantes y realizar las respectivas validaciones de antecedentes judiciales, fiscales, académicos entre otros que garanticen un uso responsable y confiable de los activos de información. ✓ Se debe aclarar al nuevo funcionario sobre los términos y condiciones de contratación al igual que del manejo y uso responsable y eficiente de los activos informáticos. ✓ El jefe inmediato o compañeros deben informar oportunamente de algún comportamiento sospechoso, incumplimiento de funciones u omisión de las mismas a la oficina de recursos humanos para establecer posibles sanciones o despidos. ✓ Es responsabilidad de los funcionarios solucionar inconvenientes dentro de su entorno laboral dentro del cumplimiento de sus funciones asignadas o solicitar apoyo de otros departamentos si así se requiere Responsabilidades de gestión. ✓ Es responsabilidad del departamento de sistemas realizar una concienciación, educación y capacitación en seguridad de la información de los activos de la información a los funcionarios del área administrativa y de historias clínicas la cual debe estar certificada por un funcionario del departamento de sistemas y cuyo informe debe ser remitido en un término no mayor a 24 horas a la oficina de recursos humanos. ✓ Los funcionarios que sean sorprendidos cometiendo actos que atenten contra el manual de procedimiento o contra la seguridad de los activos de la información en cualquiera de sus clasificaciones tendrán derecho un proceso disciplinario realizado por la oficina de recursos humanos quienes determinaran las sanciones o acciones pertinentes antes el caso.	
Responsables	Funcionarios de oficinas administrativas, funcionarios de historias clínicas, recursos humanos, departamento de sistemas, dirección general.

Sanciones	Memorando, suspensión temporal del cargo, retiro del cargo

Fuente: Autor

Tabla 24. Políticas de seguridad de gestión de activos.

Política	**7. Políticas de seguridad de gestión de activos.**
Objetivo	Definir procesos por los cuales se garantiza la protección adecuada de los activos de información.
Aplicabilidad	Dirigida a los funcionarios del departamento de sistemas, gerencia, recursos humanos, y de historias clínicas del Hospital San Francisco de Gachetá.
Directrices específicas:	
✓ El departamento de sistemas del Hospital San Francisco de Gachetá mantendrá un inventario actualizado con todos los activos de información en sus diferentes clasificaciones en el cual se especificará el responsable del uso y cuidado para el cumplimiento de funciones en el área administrativa y de historias clínicas de la entidad. ✓ Cada funcionario se hace responsable del uso adecuado de los diferentes activos informáticos así como de informar de manera oportuna anomalías en su funcionamiento o contenido al departamento de sistemas y jefe inmediato. ✓ Cada activo informático físico contará con una placa para su identificación y este debe estar en el lugar destinado para el ejercicio de sus funciones y no podrá ser transferido a otro departamento u oficina salvo autorización escrita (física o digital) del departamento de sistemas. ✓ Los activos informáticos no tendrán un uso diferente para el cual han sido adquiridos, queda prohibido la realización de actividades personales diferentes a las requeridas por el Hospital San Francisco de Gachetá.	
Responsables	Funcionarios de oficinas administrativas, funcionarios de historias clínicas, recursos humanos, departamento de sistemas, dirección general.
Sanciones	Llamado de atención, memorando, retiro del cargo.

Fuente: Autor

Tabla 25. Políticas de seguridad de control de acceso

Política	**8. Políticas de seguridad de control de acceso**
Objetivo	Asegurar un acceso controlado, físico o lógico, a los activos informáticos del Hospital San Francisco de Gachetá.
Aplicabilidad	Dirigida a los funcionarios del departamento de sistemas,

	gerencia, recursos humanos, y de historias clínicas del Hospital San Francisco de Gachetá.

Directrices específicas:

✓ El Hospital San Francisco de Gachetá dotará a los funcionarios y contratistas de todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones dentro del área administrativa y de historias clínicas para las cuales fueron contratados.

✓ Se prohíbe la instalación a la red del hospital de cualquier dispositivo electrónico ajeno al inventario que no sean autorizados por el departamento de sistemas del hospital San Francisco de Gachetá, dentro de los cuales están: teléfonos móviles, computadores portátiles, tablets, y demás elementos parecidos.

✓ El departamento de sistemas del Hospital San Francisco de Gachetá proveerá a los funcionarios las claves pertinentes para el acceso a los servicios de red y sistemas de información, estas claves son de uso personal e intransferible y es responsabilidad del usuario el manejo que se las mismas, quien trasfiera la contraseña a un tercero se verá involucrado en un proceso disciplinario o legal según el riesgo que represente este acto

✓ Tan solo el personal del departamento de sistemas podrá realizar la instalación de software o hardware en los equipos, servidores e infraestructura de tecnológica y de comunicaciones del Hospital San Francisco de Gachetá.

✓ Todo requerimiento que utilice los servidores del Hospital San Francisco de Gacheta con información de la entidad, o de sus funcionarios, no se podrá realizar de tipo remoto sin la debida aprobación del departamento de sistemas, dicha aprobación debe estar soportada por un informe de técnico de seguridad de transferencia de información elaborado y firmado por el jefe del departamento de sistemas.

✓ Se debe capacitar y controlar que los funcionarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.

✓ Los usuarios son responsables del manejo de contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá.

✓ Queda prohibida la escritura de las claves dentro de los activos de información, por ejemplo documentos digitales, correos electrónicos, bases de datos entre otros

✓ La modificación cambio o reasignación de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato previa solicitud escrita con firma física o firma digital. ✓ Se impedirá el acceso a cualquier funcionario que haya intentado el ingreso, sin éxito, a un equipo, sistema o archivo informático, en forma consecutiva por tres veces. ✓ Solo los funcionarios del departamento de sistemas podrán desbloquear el acceso a un funcionario cuya clave haya sido ingresada sin éxito con previo estudio del incidente presentado al funcionario.	
Responsables	Funcionarios de oficinas administrativas, funcionarios de historias clínicas, recursos humanos, departamento de sistemas, dirección general.
Sanciones	Suspensión temporal del cargo, retiro del cargo.

Fuente: Autor

Tabla 26. Políticas de seguridad física y ambiental.

Política	**9. Políticas de seguridad física y ambiental.**
Objetivo	Garantizar la seguridad física y ambiental de los activos de información del Hospital San Francisco de Gachetá
Aplicabilidad	Su aplicabilidad está destinada al departamento de infraestructura, departamento de sistemas, funcionarios del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá.
Directrices específicas:	
✓ El departamento de infraestructura debe garantizar la seguridad estructural de los lugares donde serán instalados los activos de información. ✓ La dirección del Hospital San Francisco de Gachetá asignara a una empresa de vigilancia un contrato del servicio de seguridad para establecer controles físicos de entrada, seguridad de oficinas, despachos y recursos. ✓ La dirección del Hospital San Francisco de Gachetá en coordinación con el departamento de sistemas realizara la adquisición de seguros contra amenazas externas y ambientales que potencialmente pueden afectar a los activos informáticos. ✓ El departamento de sistemas verificara de manera periódica situaciones relacionadas con emplazamiento y protección de equipos, seguridad del cableado y	

mantenimiento de los equipos generando un reporte de la situación presentada y apoyados por reportes entregados de manera verbal o escrita por parte de los funcionarios del área administrativa y de historias clínicas del hospital. ✓ En los lugares donde se encuentren almacenados equipos como servidores o conglomeraciones de cableado, se prohíbe fumar, comer o beber; de igual forma se prohíbe el almacenamiento de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio. ✓ Los cables deben estar marcados para identificar fácilmente los elementos conectados y evitar interrupciones del servicio, también beben existir planos que describan las conexiones del cableado. ✓ Los funcionarios del área administrativa y de historias clínicas deberán bloquear sus equipos al momento de levantarse de su puesto de trabajo para evitar alteraciones a la integridad de los activos de información necesarios para el cumplimiento de sus funciones.	
Responsables	Departamento de infraestructura, departamento de sistemas, funcionarios del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá.
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo.

Fuente: Autor

Tabla 27. Políticas de seguridad en la operativa

Política	**10. Políticas de seguridad en la operativa**
Objetivo	Asegurar la operatividad de los activos de información de acuerdo a las amenazas a las que se exponen los activos informáticos de la organización
Aplicabilidad	Dirigida a los funcionarios del departamento de sistemas, gerencia, recursos humanos, y de historias clínicas del Hospital San Francisco de Gachetá
Directrices específicas:	
✓ El departamento de sistemas garantizará según sus estrategias de seguridad la prohibición de la instalación de programas ajenos a los requeridos por los funcionarios para el cumplimiento misional y visional de la institución. ✓ El departamento de sistemas establecerá una programación para realizar copias de seguridad, semanales, mensuales, bimestrales y anuales de los activos de información del área administrativa y de historias clínicas con el fin de garantizar su disponibilidad, confidencialidad e integridad ante cualquier impacto de	

amenazas y en concordancia con los requerimientos de la entidad Hospitalaria. ✓ El departamento de sistemas solicitará a las directivas del hospital licitar con empresas especializas al menos 2 veces al año y al menos una vez por semestre pruebas de Pentesting con el fin de gestionar soluciones a posibles vulnerabilidades encontradas en el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá

Responsables	Funcionarios de oficinas administrativas, funcionarios de historias clínicas, recursos humanos, departamento de sistemas, dirección general.
Sanciones	Suspensión temporal del cargo, retiro del cargo.

Fuente: Autor

Tabla 28. Políticas de seguridad en las redes y telecomunicaciones.

Política	**11. Políticas de seguridad en las redes y telecomunicaciones.**
Objetivo	Asegurar el tráfico y envío de activos información y activos informáticos de la red del Hospital San Francisco de Gachetá.
Aplicabilidad	Dirigida a los funcionarios del departamento de sistemas, gerencia, recursos humanos, y de historias clínicas del Hospital San Francisco de Gachetá.
Directrices específicas:	
✓ Los funcionarios están obligador a utilizar de manera razonable el Internet y con propósitos laborales. ✓ Todos los funcionarios del Hospital San Francisco de Gachetá tienen prohibido el ingreso a sitios con contenidos contrarios a los propósitos misionales y visiónales de la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la organización, en caso de evidenciarse este comportamiento se procederá con el proceso disciplinario o legal al que haya lugar. ✓ Las descarga de archivos de internet que realicen los funcionarios deben responder a propósitos laborales y esto debe hacerse de forma razonable para no afectar el servicio de Internet/Intranet. ✓ El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para funcionarios cuyos propósitos de sus funciones sean facilitar canales de comunicación con la comunidad de la región del Guavio que atiende el Hospital San Francisco de Gachetá.	

✓ El Hospital San Francisco de Gachetá no se hace responsable por información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador, que sea creado a nombre personal, como redes sociales, twitter®, facebook®, youtube® likedink® o blogs, ya que se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que haya generado dichas publicaciones en los diferentes medios.

✓ No se permite el ingreso al centro de almacenamiento de servidores y demás equipos vitales para la red al personal que no esté expresamente autorizado. El departamento de sistemas debe llevar un control de ingreso y salida del personal que visita el centro de datos sin excepción e ideara la manera más oportuna y segura de llevar dichos registros atendiendo los parámetros de calidad de la organización.

✓ El departamento de sistemas y el departamento de infraestructura del hospital San Francisco de Gachetá deberán garantizar que todos los equipos de los centros de datos del área administrativa y de historias clínicas cuenten con un sistema alterno de respaldo de energía ante las frecuentes fallas eléctricas de la región.

✓ El departamento de sistemas en coordinación con la oficina de recursos humanos programaran capacitaciones al personal de aseo sobre la forma en que se debe realizar la limpieza externa de los equipos que hacen parte de los activos de red del Hospital San Francisco de Gachetá.

✓ Los funcionarios tiene prohibido ingerir alimentos o bebidas cerca de los activos informáticos, también tienen prohibido acceder a ellos bajo los efectos de sustancias psicoactivas.

✓ Es obligación de los funcionarios reducir la presencia de elementos como papel y cualquiera que pueda representar riesgo de propagación de fuego, se debe mantener organizado el puesto de trabajo.

✓ El departamento de infraestructura y el departamento de sistemas garantizara que las zonas de disposición de los activos de información estén provistos de:

- Señalización apropiada de todos y cada uno de los diferentes equipos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.

- Pisos construidos con materiales no inflamables.

- Sistema de refrigeración por aire acondicionado de precisión.

- Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.

- Se debe garantizar el servicio de fluido eléctrico de manera constante y eficaz, se debe instalar en cada uno de los equipos una UPS para mitigar fallas en el servicio de energía.

- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario del departamento de sistemas del hospital san Francisco de Gachetá

- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales, el departamento de infraestructura deberá verificar las fechas de vencimiento y elaborará un plan para garantizar la disponibilidad ante una emergencia.

- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan y que el montaje de este no afecte la movilidad de usuarios y funcionarios.

- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas, el montaje de estos no afecte la movilidad de usuarios y funcionarios.

- Las puertas de acceso a lugares donde se encuentren activos de información importantes para el área administrativa y de historias clínicas deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro hospitalario.

- Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad, dicha función dependerá de un funcionario del departamento de sistemas.

- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.

• Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.	
Responsables	Funcionarios de oficinas administrativas, funcionarios de historias clínicas, recursos humanos, departamento de sistemas, dirección general.
Sanciones	Llamado de atención, memorando, suspensión temporal del cargo, retiro del cargo.

Fuente: Autor

- **CUMPLIMIENTO**

Los diferentes aspectos descritos en este documento son de obligatorio cumplimiento para todos los funcionarios del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá. En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, el Hospital San Francisco de Gachetá tomará las acciones disciplinarias y legales correspondientes.

11. SGSI HOSPITAL SAN FRANCISCO DE GACHETÁ.

Para el diseño del sistema de gestión de seguridad informática en el Hospital San Francisco de Gachetá se han establecido el desarrollo de 4 fases que permiten el correcto y pertinente cumplimiento de las políticas de seguridad para la aplicación de controles ISO 27001 27002 de acuerdo con los análisis de amenazas y valoración del riesgo mostrado anteriormente según los cuales se han establecido políticas de seguridad que respondan a la aplicación de controles ISO cumpliendo con unos objetivos por política de seguridad y de acuerdo a unas responsabilidades asignadas.

Dentro del diseño del sistema de gestión de seguridad informática para el hospital San Francisco de Gachetá se plantean 4 fases que guiaran el proceso en una futura implementación del presente diseño, lo anterior significa que la propuesta de diseño contempla elementos que le permitirán al Hospital San Francisco de Gachetá proceder con la implementación real de la propuesta.

Las 4 fases necesarias para el Sistema De Gestión de Seguridad Informática del hospital San Francisco de Gachetá son:

- FASE 1: Planificar: Análisis diferencial y de riesgos para definición del alcance y otras actividades de planeación.

- FASE 2: Hacer: Propuesta para implantar el diseño del SGSI

- FASE 3: Verificar: Seguimiento, supervisión y revisión del SGSI

- FASE 4: Actuar: Mantener y mejorar el sistema

A continuación se presenta el diseño de cada una de las fases anteriormente mencionadas donde se muestran los diferentes requerimientos para el diseño del sistema de gestión de seguridad informática teniendo en cuenta los dominios seleccionados y las políticas de seguridad informática creadas en el presente documento, adicionalmente se plantea una propuesta de implementación, verificación y mejora del sistema de gestión de seguridad informática en una posible implementación de la propuesta, lo anterior como valor agregado teniendo en cuenta que este proyecto está dirigido al diseño del SGSI.

11.1 FASE 1: PLANIFICAR: ANÁLISIS DIFERENCIAL Y DE RIESGOS PARA DEFINICIÓN DEL ALCANCE Y OTRAS ACTIVIDADES DE PLANEACIÓN.

Tras el análisis realizado de amenazas y junto con su la respectiva valoración del riesgo se han establecido una serie de controles de acuerdo a la Norma ISO 27001-27002, de acuerdo a esto se han creado políticas de seguridad las cuales tienen como fin garantizar la seguridad de los activos de información del Hospital San Francisco de Gachetá en sus diferentes dimensiones, por lo anterior es necesario elaborar un análisis diferencial concretando así un informe actual de los controles propuestos para estandarizar responsabilidades para una futura implementación del diseño sistema de seguridad informática en la entidad hospitalaria presentado en este documento.

A continuación se relaciona el análisis diferencial de los controles ISO propuestos para el Hospital San Francisco de Gachetá donde se realiza una revisión de cada uno de los controles propuestos y se expone el estado de los mismos ya que en algunos pasos se ha dado una implementación básica con otros fines cuyo avance puede ser importante para la propuesta del diseño del SGSI para la entidad:

Tabla 29. Análisis diferencial de los controles ISO 207001-27002 para el Hospital San Francisco de Gachetá

SECCION – CONTROL	ESTADO	RESPONSABLE	OBSERVACIONES
5.1 Directrices de la Dirección en seguridad de la información			
5.1.1 Conjunto de políticas para la seguridad de la información.	Sin implementar	• Departamento de sistemas. • Funcionarios del área administrativa y de historias clínicas. • Gerencia. • Recursos humanos.	Se deben implementar de acuerdo a lo solicitado en el diseño.
6.1 Organización interna			
6.1.1 Asignación de responsabilidades para la seguridad de la información.	Sin implementar	• Departamento de sistemas. • Funcionarios del área administrativa y de historias clínicas. • Gerencia. • Recursos humanos.	Las responsabilidades deben asignarse de acuerdo al perfil y la función realizada
6.1.3 Contacto con las autoridades.	Implementado	• Departamento de sistemas. • Funcionarios del área administrativa y de historias clínicas.	Se deben establecer tiempos de respuesta y procedimientos acordes con la ISO 207002

		• Gerencia. • Recursos humanos.	
7.1 Antes de la contratación.			
7.1.1 Investigación de antecedentes.	Implementado	• Gerencia • Recursos humanos	Sin observaciones
7.1.2 Términos y condiciones de contratación.	Parcialmente implementado	• Gerencia • Recursos humanos	Se deben incluir aspectos acerca del manejo y protección de activos informáticos.
7.2 Durante la contratación.			
7.2.1Responsabilidades de gestión.	Implementado	• Departamento de sistemas • Funcionarios del área administrativa y de historias clínicas. • Gerencia • Recursos humanos	Las responsabilidades deben asignarse de acuerdo al perfil y la labor realizada
7.2.2 Concienciación, educación y capacitación en seguridad de la información.	Sin implementar	• Departamento de sistemas • Gerencia • Recursos humanos	Se debe realizar la capacitación teniendo en cuenta el diseño propuesto para el SGSI.

7.2.3 Proceso disciplinario	Implementado	• Gerencia • Recursos humanos	Sin observaciones
8.1 Responsabilidad sobre los activos			
8.1.1 Inventario de activos.	Implementado	• Departamento de sistemas.	Mejorar teniendo en cuenta las clasificaciones de los activos informáticos.
8.1.2 Propiedad de los activos.	Implementado	• Departamento de sistemas.	Sin observaciones
8.1.3 Uso aceptable de los activos.	Sin implementar	• Departamento de sistemas • Funcionarios del área administrativa y de historias clínicas.	Aplicar políticas de uso aceptable de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá.
9.3Responsabilidades del usuario.			
9.3.1 Uso de información confidencial para la autenticación.	Sin implementar	• Departamento de sistemas • Funcionarios del área administrativa y de historias clínicas. • Gerencia.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá.
9.4 Control de acceso a sistemas y aplicaciones.			

9.4.1 Restricción del acceso a la información.	Sin implementar	• Departamento de sistemas, • Departamento de infraestructura • Funcionarios del área administrativa y de historias clínicas. • Gerencia.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá.
9.4.2 Procedimientos seguros de inicio de sesión.	Parcialmente implementado	• Departamento de sistemas • Funcionarios del área administrativa y de historias clínicas, • Gerencia.	Mejorar procedimiento de inicio de sesión con la implementación de contraseñas de mejor nivel de seguridad y mejor protocolo de inicio de acuerdo a las políticas del diseño
9.4.3 Gestión de contraseñas de usuario	Sin implementar	• Departamento de sistemas • Funcionarios del área administrativa y de historias clínicas, • Gerencia.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá y verificar la gestión de contraseñas por parte de los funcionarios
11.1 Áreas seguras.			
11.1.1 Perímetro de seguridad física.	Sin implementar	• Departamento de sistemas. • Departamento de infraestructura. • Gerencia.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá para el control de acceso.

11.1.2 Controles físicos de entrada.	Sin implementar	• Departamento de sistemas • Departamento de infraestructura. • Gerencia.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá para el control de acceso.
11.1.3 Seguridad de oficinas, despachos y recursos.	Parcialmente implementado	• Departamento de sistemas • Departamento de infraestructura • Gerencia.	Mejorar los protocolos de ingreso a espacios físicos de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá para el control de acceso.
11.1.4 Protección contra las amenazas externas y ambientales.	Parcialmente implementado	• Departamento de infraestructura • Gerencia.	Aplicar procedimientos de control de riesgo residual de acuerdo a las políticas del diseño de implementación del SGSI.
11.1.5 El trabajo en áreas seguras.	Parcialmente implementado	• Departamento de infraestructura. • Gerencia. • Recursos humanos.	Realizar ajustes al procedimiento actual con respecto al diseño de implementación del SGSI para el Hospital San Francisco de Gachetá.
11.1.6 Áreas de acceso público, carga y descarga.	Sin implementar	• Departamento de infraestructura. • Gerencia. • Departamento de sistemas	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá
11.2 Seguridad de los equipos.		•	
11.2.1 Emplazamiento y protección de equipos.	Sin implementar	• Departamento de Sistemas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI

		• Gerencia.	para el hospital San Francisco de Gachetá
11.2.3 Seguridad del cableado.	Parcialmente implementado	• Departamento de infraestructura. • Departamento de sistemas	Verificar las conexiones eléctricas y de datos para validar la certificación de las mismas
11.2.4 Mantenimiento de los equipos	Implementado	• Departamento de sistemas	Mejorar los protocolos de seguridad en los procesos de mantenimiento de acuerdo a la ISO 27001 - 27002
11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.	Sin implementar	• Departamento de Sistemas. • Gerencia.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá
11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento	Sin implementar	• Departamento de Sistemas. • Funcionarios del área administrativa y de historias clínicas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá
11.2.8 Equipo informático de usuario desatendido.	Sin implementar	• Departamento de Sistemas. • Funcionarios del área administrativa y de historias clínicas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá
11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.	Sin implementar	• Departamento de Sistemas. • Funcionarios del área administrativa y de historias clínicas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá

12.2 Protección contra código malicioso.			
12.2.1 Controles contra el código malicioso.	Sin implementar	• Departamento de Sistemas. • Funcionarios del área administrativa y de historias clínicas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá de acuerdo a las redes y telecomunicaciones.
12.3 Copias de seguridad.			
12.3.1 Copias de seguridad de la información.	Parcialmente implementado	• Departamento de Sistemas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá de acuerdo al manejo de los activos de información
12.4 Registro de actividad y supervisión.			
12.4.1 Registro y gestión de eventos de actividad.	Sin implementar	• Departamento de Sistemas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá de acuerdo a lo establecido para seguridad de los activos informáticos
12.5 Control del software en explotación.			
12.5.1 Instalación del software en sistemas en producción.	Parcialmente implementado	• Departamento de Sistemas.	Mejorar los protocolos de instalación de programas teniendo en cuenta la pertinencia

			de la instalación de los mismos para las funciones de los empleados
12.6 Gestión de la vulnerabilidad técnica.			
12.6.1 Gestión de las vulnerabilidades técnicas	Parcialmente implementado	• Departamento de Sistemas.	Mejorar los protocolos de tratamiento de vulnerabilidades aplicando en menores tiempos pruebas de seguridad de la información con empresas especializadas.
12.6.2 Restricciones en la instalación de software.	Sin implementar	• Departamento de Sistemas.	Establecer protocolos para la instalación pertinente de programas de acuerdo a las funciones del empleado impidiendo la instalación de programas por personal ajeno al del departamento de sistemas.
13.1 Gestión de la seguridad en las redes.			
13.1.1 Controles de red.	Sin implementar	• Departamento de Sistemas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá de acuerdo a las redes y telecomunicaciones.
13.1.2 Mecanismos de seguridad asociados a servicios en red.	Sin implementar	• Departamento de Sistemas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de

			Gachetá de acuerdo a las redes y telecomunicaciones.
13.1.3 Segregación de redes.	Sin implementar	• Departamento de Sistemas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá de acuerdo a las redes y telecomunicaciones.
13.2 Intercambio de información con partes externas.			
13.2.4 Acuerdos de confidencialidad y secreto.	Sin implementar	• Departamento de Sistemas. • Recursos humanos. • Gerencia • Funcionarios del área administrativa y de historias clínicas	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá de acuerdo los protocolos del diseño para acuerdos de confidencialidad.
14.1 Requisitos de seguridad de los sistemas de información.			
14.1.1 Análisis y especificación de los requisitos de seguridad	Sin implementar	• Departamento de Sistemas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá de acuerdo a las directrices de instalación de software

14.2 Seguridad en los procesos de desarrollo y soporte.	Sin implementar	• Departamento de Sistemas.	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá de acuerdo a las redes y telecomunicaciones y activos de la información.
14.2.1 Política de desarrollo seguro de software	Sin implementar	• Departamento de Sistemas. • Gerencia	Aplicar políticas de acuerdo a la propuesta de diseño de SGSI para el hospital San Francisco de Gachetá.

Fuente: Autor

11.2 FASE 2: HACER: PROPUESTA PARA IMPLANTAR EL DISEÑO DEL SGSI

Para poder realizar la implementación del diseño SGSI en el hospital San Francisco de Gachetá deben realizarse una serie de pasos los cuales se relacionan a continuación:

- **Aplicación de los controles ISO 27001- 27002 de acuerdo a las políticas de seguridad propuesta en el diseño.** Deben aplicarse las políticas y procedimientos dentro del alcance del SGSI, que para el caso del Hospital San Francisco de Gachetá podrán ser globales o sectoriales o específicas estas últimas aplicadas al área administrativa y de historias clínicas del hospital San Francisco de Gachetá.

Se debe verificar una vez más que las políticas establecidas en el diseño no alteren el manual de procedimientos en alto nivel al momento de ejecutar los procesos, esto podrá generar interrupción en el servicio a los pacientes por lo que será necesario hacer una lista de chequeo previo a la implementación del diseño, para esto podrán revisarse los análisis de amenazas, la valoración del riesgo, las políticas propuestas y el análisis diferencial elaborado al Hospital San Francisco de Gachetá.

Las políticas, controles y procedimientos deben ser adecuadamente comunicados e impulsados para su revisión y aplicación verificando el cumplimiento de los mismos.

Con lo anteriormente mencionado se deben tener en cuenta los siguientes aspectos:

a. Alcance del SGSI para el Hospital San Francisco de Gachetá.

b. Resultado de la evaluación de Riesgos para el Hospital San Francisco de Gachetá.

c. Política del SGSI para el Hospital San Francisco de Gachetá.

d. Declaración de aplicabilidad de acuerdo a la ISO 27001-27002.

e. Plan de Tratamiento de Riesgos según los controles asignados.

f. Marco Legal, Normativo y Regulatorio de acuerdo a las leyes colombianas y al manual de procedimiento de la entidad.

g. Garantizar la participación de personal con capacitación en el proceso como ingenieros con conocimientos en seguridad informática, ingenieros con conocimientos y certificaciones en normas ISO.
h. Asignar responsabilidades y verificar el cumplimiento de las mismas al personal involucrado en el proceso.

- **Implementación de controles.** Tras verificar los activos informáticos se han determinados amenazas que pueden afectarlos, adicionalmente a esto, se han establecido las diferentes valoraciones del riesgo y como resultado de esto se han propuesto los controles en el diseño del SGSI para el hospital San Francisco de Gachetá.

Para el proceso de implementación del diseño de esta propuesta se sugiere que se documente de manera más detallada cada uno de los controles para así determinar recursos económicos, técnicos, planes de capacitación entre otras necesarias para su completo y óptimo desarrollo.

Adicionalmente a esto se debe garantizar la armonización entre las partes involucradas (departamento de sistemas, gerencia, departamento de infraestructura recursos humanos, área administrativa y de historias clínicas) para que todos en conjunto entiendan el proceso y cooperen ante posibles incidentes que se presenten con los activos de información.

Se propone crear el comité de Seguridad Informática el cual este presidido por el jefe del departamento de sistemas y al menos un representante de las demás áreas involucradas en el diseño de SGSI del hospital San Francisco de Gachetá.

Finalmente es importante que se asignen responsabilidades y se generen cronogramas con fechas y procesos para la implementación de los controles que se proponen en esta propuesta de diseño.

- **Implementación de un programa de sensibilización y capacitación.** Las capacitaciones son importantes ya que estas garantizaran que todos los sectores e individuos involucrados dentro del proceso conozcan las políticas de seguridad que deben cumplir dentro del desarrollo de sus funciones ya que al momento de presentarse un incidente el desconocimiento de procesos no será una causa que se presente en un alto porcentaje.

Lo anterior permitirá acciones como:

- Incidentes por desconocimiento del proceso.
- Evitar rechazos a la implementación del proceso.
- Preparar al personal a nivel conceptual y práctico.
- Facilitar la implementación del diseño de esta propuesta.

Todos los sectores involucrados tienen la obligación de responder a incidentes de seguridad informática y todos deben cooperar con la mitigación de riesgos mejorando los procesos de manera directa o indirecta en lo relacionado con la seguridad de los activos informáticos.

- **Implementación de un programa de gestión de incidentes.** Es importante realizar la documentación de los diferentes incidentes de seguridad de los activos de información que se presentan dentro del Hospital San Francisco de Gachetá, esto debe responder a mitigar los incidentes y disminuir la probabilidad de una nueva ocurrencia.

Además de un monitoreo de incidentes y cumplimiento de las políticas de seguridad es importante que se genere un manual de procesos donde se proponga o establezcan las acciones a seguir para enfrentar un incidente por lo que se propone para la entidad:

- Establecer como reportar el incidente
- Formas de escalonamiento
- Plan de contingencia
- Acciones reparatorias
- Priorización de incidentes y áreas de trabajo afectadas
- Recolección de evidencias
- Comunicar en el menor tiempo posible a usuarios afectados
- Presentar informe mensual o trimestral a la gerencia
- Levantar estadísticas de los incidentes presentados
- Generar auditorías internas para el SGSI verificando el cumplimiento de las políticas de seguridad y el alcance de los indicadores propuestos para mitigar el riesgo.

- **Gestión de recursos para el SGSI.** Para implementar el SGSI en el Hospital se requiere de una serie de recursos económicos, tecnológicos y humanos.

Con el fin de optimizar este tipo de recursos se debe acudir al análisis del costo beneficio, es decir que se debe priorizar las inversiones de acuerdo a la necesidad insatisfecha en lo relacionado con la seguridad de los activos de información.

Una vez determinadas las prioridades se debe elaborar un plan de asignación de recursos que para este caso particular deben ser tecnológicos y humanos para responder a la inversión requerida cumpliendo así con las políticas de seguridad garantizando la aplicación prioritaria de los controles seleccionados para los activos informáticos que se determinen que están en alto riesgos y cuya afectación dañara considerablemente el proceso de atención apacientes dentro del hospital.

Finalmente esta priorización de gastos será elaborada con previa autorización de la gerencia acompañada de un informe del departamento de sistemas el cual se elaborara teniendo en cuenta esta propuesta de diseño de SGSI para el Hospital San Francisco.

11.3 FASE 3: VERIFICAR: SEGUIMIENTO, SUPERVISIÓN Y REVISIÓN DEL SGSI

Siempre será necesario evaluar los procesos que se dan dentro de una organización, el proceso de verificación permitirá ajustar las propuestas del diseño con relación a la situación real ya que a pesar de que se ha partido de un análisis real en alguno casos las propuestas o los controles pueden verse desfasados o ser muy estrictos lo cual puede alterar la armonía institucional o generar un mayor sobrecosto en el proceso.

Este proceso de verificación debe realizarse de acuerdo al cumplimiento de los controles ISO 27001-27002 versión 2013 que se han seleccionado para el Hospital San Francisco de Gachetá, esto debe realizarse de manera periódica y de primera mano será responsabilidad del departamento de sistemas quienes de ser necesario solicitaran a la gerencia una licitación para contratar una revisión externa de una empresa especializada y certificada en el tema.

Para realizar un proceso de verificación efectivo el departamento de sistemas debe realizar las siguientes actividades:

- **Monitoreo.** Se debe realizar con el fin de establecer anomalías en relación con las políticas y el cumplimiento de las mismas dentro del proceso real dentro del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá.

Este monitoreo será responsabilidad del departamento de sistemas y se ejecutara de acuerdo a lo controles implementados en cada uno de los activos de información de la entidad y se realizara de acuerdo a un plan de monitoreo que responda a la prevención oportuna de posibles amenazas por el incumplimiento de las políticas de seguridad.

Tabla 30. Cronograma de monitoreo

CONTROL	SEMANA				RESPONSABLE
	1	2	3	4	
11.1.2 Controles físicos de entrada.					Gerencia – Celaduría
11.1.3 Seguridad de oficinas, despachos y recursos.					Funcionarios- celaduría
11.1.4 Protección contra las amenazas externas y ambientales.					Departamento de sistemas
11.1.5 El trabajo en áreas seguras.					Departamento de infraestructura

11.2.4 Mantenimiento de los equipos.					Departamento de sistemas
12.1.2 Gestión de cambios.					Gerencia.
12.2.1 Controles contra el código malicioso.					Departamento de sistemas
12.6.1 Gestión de las vulnerabilidades técnicas.					Departamento de sistemas
12.3.1 Copias de seguridad de la información.					Departamento de sistemas
12.6.2 Restricciones en la instalación de software.					Departamento de sistemas
13.1.1 Controles de red.					Departamento de sistemas
13.2.1 Políticas y procedimientos de intercambio de información.					Departamento de sistemas
13.1.2 Mecanismos de seguridad asociados a servicios en red.					Departamento de sistemas
13.2.4 Acuerdos de confidencialidad y secreto.					Gerencia – Recursos Humanos
14.2.4 Restricciones a los cambios en los paquetes de software.					Departamento de sistemas
14.2.2 Procedimientos de control de cambios en los sistemas.					Departamento de sistemas
16.1.2 Notificación de los eventos de seguridad de la información.					Departamento de sistemas
14.2.9 Pruebas de aceptación.					Departamento de sistemas
14.2.5 Uso de principios de ingeniería en protección de sistemas.					Departamento de sistemas
7.2.2 Concienciación, educación y capacitación en seguridad de la información.					Departamento de sistemas-Recursos Humanos
6.1.1 Asignación de responsabilidades para la seguridad de la información.					Departamento de sistemas
7.2.1 Responsabilidades de gestión.					Gerencia
8.2.2 Etiquetado y manipulado de la información.					Departamento de sistemas
8.1.1 Inventario de activos.					Departamento de sistemas

8.1.3 Uso aceptable de los activos.					Departamento de sistemas
9.4.1 Restricción del acceso a la información.					Departamento de sistemas
9.4.1 Restricción del acceso a la información.					Departamento de sistemas
9.1.1 Política de control de accesos.					Departamento de sistemas
9.2.2 Gestión de los derechos de acceso asignados a usuarios.					Departamento de sistemas

Fuente: Autor

- **Métricas.** El departamento de sistemas en conjunto con la gerencia debe establecer una serie de indicadores, esto permitirá establecer evaluaciones y asignar valores al cumplimiento de los controles establecidos según la política de seguridad de la información.

Cabe resaltar que con el plan de indicadores y la verificación del mismo se podrá determinar si el control satisface la necesidad de seguridad en cada uno de los activos informáticos o por el contrario se excede en su aplicación o es insuficiente, para este último caso se debe replantear el control ya que representa una amenaza latente que en caso de materializarse en un incidente negativo puede afectar seriamente el proceso de atención oportuna a pacientes del Hospital San Francisco de Gachetá.

- **Auditorías internas y externas** No siempre la opinión y procesos que se realicen por parte del personal interno es el más adecuado por lo que es importante recurrir a la opinión de terceros, por lo anterior se deben implementar auditorías internas y externas dentro de intervalos de tiempo debidamente planificados cumpliendo así con lo solicitado por el estándar ISO 27001-27002 en lo relacionado con auditorías a los controles, para tal fin los procesos de auditoria están llamados a verificar:

a. Requisitos de la norma implantada, la legislación y reglamentaciones con las que se han implementado las políticas de seguridad.
b. Que existan los requisitos necesarios para ejecutar las políticas de seguridad de la información dentro del Hospital San Francisco de Gachetá.
c. Verificar que los controles seleccionados estén implementados de manera correcta y respondan a las necesidades de seguridad de los activos de información.
d. Verificar la eficiencia de cada uno de los controles implementados y su ejecución para mitigar el nivel de los riesgos de acuerdo a las amenazas encontradas para los activos informáticos.

Lo anterior responde a alguna metodología de auditoria que pueda aplicarse a esta propuesta de diseño de SGSI para el Hospital San Francisco de Gachetá

- **Revisión** Los procesos de revisión deben realizarse de manera programada y periódica, es responsabilidad del departamento de sistemas generar esta planeación y dar cumplimiento a las acciones de revisión dentro de los tiempos establecidos por la entidad, para este proceso de revisión es importante realizar los siguientes procesos:

a) Valorar la efectividad del SGSI en la mitigación del riesgo
b) Analizar y valorar los recursos económicos, humanos y tecnológicos asignado al SGSI del Hospital San Francisco de Gachetá
c) Considerar los riesgos residuales y establecer procedimientos para mitigar su impacto.
d) Renovar los planes de seguridad de acuerdo a las últimas actualizaciones de la ISO para responder a amenazas futuras.

Tabla 31. Calendario de evaluación de SGSI.

PROCESO	Meses												RESPONSABLES
	1	2	3	4	5	6	7	8	9	10	11	12	
Valorar la efectividad del SGSI en la mitigación del riesgo.													Gerencia – Departamento de sistemas
Analizar y valorar los recursos económicos, humanos y tecnológicos.													Gerencia, Recursos humanos, Departamento de sistemas
Considerar los riesgos residuales y establecer procedimientos para mitigar su impacto.													Gerencia – Departamento de sistemas
Renovar los planes de seguridad de acuerdo a las últimas actualizaciones de la ISO para responder a amenazas futuras.													Gerencia – Departamento de sistemas

Fuente: Autor

11.4 FASE 4: ACTUAR: MANTENER Y MEJORAR EL SISTEMA

De acuerdo con las medidas tomadas y las situaciones presentadas en la fase III y teniendo en cuenta los resultados de los controles, la métrica, monitoreo, revisión y luego de implementar el SGSI en el hospital San Francisco de Gachetá se deben analizar aquellas políticas que deban reforzarse para dar solución a los incidentes presentados para replantear las políticas, procesos o establecer sanciones respectivas con el fin de cumplir en mejor nivel con la mitigación del riesgo a los que se ven enfrentados los activos informáticos del Hospital San Francisco de Gachetá del área administrativa y de historias clínicas.

Es importante que dentro de la fase 4 se planteen acciones de mantenimiento y mejora del SGSI ya que esto mitigará considerablemente la posibilidad de una materialización del riesgo ya que al verificar el funcionamiento de los diferentes

activos de información se garantiza que los procesos cumplan a cabalidad con las políticas de seguridad informática propuestas para la entidad hospitalaria y se pueda brindar un servicio de calidad con alto nivel de seguridad desde el área administrativa y de historias clínicas dispuesto a continuas mejoras.

En esta fase se deberá actuar sobre los siguientes aspectos:

- No conformidades con respecto a la aplicación de políticas del SGSI.
- Establecer acciones correctivas.
- Analizar los informes de auditoría y corregir fallos encontrados.
- Tener en cuenta sugerencias de los funcionarios del área administrativa y de historias clínicas.
- Obtener recursos que falten para optimizar el SGSI.
- Monitorear la implementación de cambios.
- Comunicar al comité de seguridad informática del Hospital San Francisco de Gachetá los posibles cambios o modificaciones que se deban realizar al SGSI.

A continuación se relaciona el formato para realizar el registro del proceso de mantenimiento:

Tabla 32. Formato de mantenimiento y mejora del SGSI del Hospital San Francisco de Gachetá

FORMATO DE MANTENIMIENTO Y MEJORA DEL SGSI DEL HOSPITAL SAN FRANCISCO DE GACHETÁ			
Proceso de:		Mantenimiento ☐	Mejora ☐
Dirigido a:	Activo ☐	Política ☐	Control ☐
Objetivo:_____ _____ _____ _____			
Responsable:_____			

Funcionario que reporta:_____	
Departamento:_____	
Inconformidad:_____ _____ _____ _____	
Acciones de mejora o mantenimiento:_____ _____ _____	
Observaciones:_____ _____ _____ _____	
Costo mano de obra:_____	
Costo Material: Si se requiere	
Implemento 1	
Implemento 2	
Implemento 3	
Implemento 4	
Implemento 5	
Implemento 6	
Total Costo final	

Fuente: Autor

11.5 Plan de continuidad del negocio Hospital San Francisco de Gachetá.

- **¿Qué es un plan de continuidad de negocio?**

Se compone de diferentes fases realizadas para analizar los procedimientos a desarrollar en caso de la materialización de amenazas una vez implementado el sistema de Gestión de seguridad informática del Hospital San Francisco de Gachetá.

Su principal objetivo es el de garantizar el funcionamiento normal de los procesos de información dentro del Hospital San Francisco de Gachetá a pesar de la materialización de una amenaza.

Para proponer el plan de continuidad del negocio se deben analizar dos situaciones principales:

- Identificar los activos de información críticos para el funcionamiento de la entidad

- Cuál es el tiempo de recuperación de los activos informáticos que se han afectado pro la materialización de la amenaza.

- **¿Por qué es importante para el SGSI del Hospital San Francisco de Gachetá?**

Dentro del diseño del SGSI se propone la elaboración del plan de continuidad del negocio como respuesta a alguna posible falla de las políticas y controles de seguridad expuestos en este documento, es decir se plantea como necesidad de respuesta ante la materialización de una amenaza constituyéndose en el plan B que se debe ejecutar desde el departamento de sistemas de la entidad hospitalaria quienes aunaran esfuerzos con integrantes de otros departamentos

para garantizar el continuo funcionamiento del servicio generando soluciones rápidas que minimicen el impacto de la amenaza materializada.

El plan de continuidad del negocio debe activarse una vez se evidencia la materialización de alguna amenaza para los activos de información del Hospital San Francisco de Gacheta, lo cual lo constituye en una herramienta fundamental para la ejecución de procesos y salvavidas importante en la prestación del servicio.

Para implementar el plan de continuidad del negocio en el Hospital San Francisco de Gachetá se han de realizar las 4 fases descritas a continuación:

- **Fase I – Análisis Del Negocio Y Evaluación De Riesgos**

En esta fase se deben identificar los principios de funcionamiento de la institución, se deben analizar los objetivos, sus principios misionales y visiónales para identificar los activos de información críticos donde al materializarse una amenaza se proceda con la activación del plan de contingencia.

- **Fase II– Selección De Estrategias**

En esta fase se debe cumplir con dos objetivos:

- Valorar estrategias de respaldo para establecer las más apropiadas que se deben implementar ante la materialización de una amenaza.

- Corregir de manera definitiva vulnerabilidades detectadas después de la implementación del SGSI.

- **Fase III- Desarrollo Del Plan**

Tras la evaluación de las diferentes estrategias de respaldo y contingencia, en esta fase se debe dar inicio a la implementación de la estrategia seleccionada con el fin de establecer el plan B para el SGSI dentro del Hospital San Francisco de Gachetá.

- **Fase IV – Pruebas Y Mantenimiento**

En esta última fase se realiza la evaluación de la estrategia de continuidad del negocio para así verificar si esta es eficaz o no, lo anterior permitirá mejorar el nivel de efectividad ante la mitigación del riesgo de materialización de amenazas para afinarlo según los resultados estableciendo un plan de mejora.

Teniendo en cuenta la información recopilada sobre el Hospital San Francisco de Gachetá y su posible análisis de riesgos y si aplicación de controles según la norma ISO 27001-27002 se elabora el plan de continuidad del negocio.

- **FASE I – ANÁLISIS DEL NEGOCIO Y EVALUACIÓN DE RIESGOS**

Análisis del negocio

Con el fin de contextualizarse acerca de las características del Hospital San Francisco de Gachetá por favor remitirse al numeral 6.2 MARCO CONTEXTUAL de este documento donde encontrar la información relacionada con este ítem.

Análisis del impacto

En esta fase se permite identificar de manera más clara los procesos misionales de cada entidad y analizar el nivel de impacto con relación a la gestión del negocio.

El Hospital San Francisco de Gachetá es una entidad financiada con recursos públicos, presta el servicio de atención en salud hasta el segundo nivel a todos los habitantes de la región del Guavio conformada por los municipios de Gachetá, Ubalá, Gama, Junín y Gachalá

Sus procesos misionales y visiónales están enfocadas en el sector salud donde se evidencia una vulnerabilidad en sector administrativo financiero y de historias clínicas del Hospital por lo que se ha elaborado el diseño de un SGSI para mitigar el riesgo y mejorar la usabilidad de los activos informáticos.

Relación de procesos

La relación de procesos se encuentra descrita en el manual de procesos y procedimientos del Hospital San Francisco de Gachetá por lo que en este documento se ha establecido una clasificación de activos informáticos que pertenecen al área administraba y de historias clínicas de la entidad.

Relación de aplicaciones

De acuerdo a las aplicaciones utilizadas en el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá se ha identificado que los activos de información como bases de datos y el aplicativo CNT programa de gestión administrativa, (programa eje del funcionamiento del hospital) constituyen el núcleo de funcionamiento informacional del historial de pacientes, por lo que de su

buena relación con los demás activos de información en lo relacionado con configuración, compatibilidad, capacitación de manejo a funcionarios entre otros dependerá que se obtenga mayor efectividad de cumplimiento de la razón misional y visional de la entidad.

Relación de departamentos y usuarios

Para conocer más a fondo el proceso de relación de departamentos y usuarios por favor remitirse a los anexos C, D y E donde encontrará los diferentes organigramas de los departamentos involucrados en el análisis del presente documento.

La dirección general del Hospital San Francisco de Gachetá junto con el Departamento de sistemas son los encargados de supervisar la ejecución de decisiones con relación a seguridad informática y la posible materialización de amenazas en los activos de información a pesar de haber implementado el sistema de gestión de seguridad informática lo cual genera un impacto como se muestra en la siguiente tabla:

Tabla 33. Impacto de procesos

Proceso	Descripción	Frecuencia	Responsable
PLANEACIÓN ESTRATÉGICA	Se encargar de realizar toda la planeación estratégica con relación a la razón misional y visional del negocio logrando el posicionamiento del Hospital San Francisco de Gachetá.	CONTINUO	Dirección General

EVALUACIÓN ESTRATÉGICA, ANÁLISIS Y MEJORA	Proceso de medición del desempeño del sistema de gestión integral, se pueden establecer procesos como auditorias para el cumplimiento de este ítem	CONTINUO	Dirección General
GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Implementación de un sistema de gestión de seguridad informática para proteger los activos de información del Hospital Sam Francisco de Gachetá.	CONTINUO	Director del departamento de seguridad informática
GESTIÓN DE OPORTUNIDADES	Gestionar otros negocios, firmar contratos de servicios, convenios y licitaciones	CONTINUO	Director Financiero
GESTIÓN DE LA EJECUCIÓN	Desarrollar los productos de acuerdo a lo requerido por el usuario, verificar la efectividad de satisfacción del servicio recibido.	CONTINUO	Director general
GESTIÓN HUMANA	Realizar contratación de personal idóneo y mantener a quien muestre los mejores rendimientos, capacitar en nuevos procesos o actualización de los mismos	CONTINUO	Responsable de recursos humanos

GESTIÓN DE RECURSOS ADMINISTRATIVOS	Gestionar los recursos físicos y económicos para el hospital. Efectuar las compras y pagos a los proveedores de la compañía. Administrar y mantener la tecnología que soporta las operaciones de la entidad. Gestionar la contabilidad de la entidad.	CONTINUO	Director financiero
GESTIÓN DOCUMENTAL	Crear, editar y distribuir los documentos necesarios para el desarrollo de los proyectos del Hospital, gestionar la correspondencia a los diferentes departamentos.	CONTINUO	Secretarios y recepcionista

Fuente: Autor

Determinar los procesos críticos

Mantenimiento de bases de datos de usuarios y programa CNT programa de gestión administrativa, (programa eje del funcionamiento del hospital).

Servidores de base de datos designados para el almacenamiento de información de las historias clínicas de los usuarios del Hospital.

Dentro del departamento administrativo financiero se generan procedimientos de inversión de capital.

El área de historias clínicas recepciona toda la información de los pacientes (Usuarios) del Hospital San Francisco de Gachetá lo cual constituye en el activo de información más importante ya que partiendo de este se genera la atención oportuna y de calidad a los pacientes cumpliendo así con la razón misional y visional de la entidad.

Para conocer las amenazas, valoración del riesgo, controles implementados entre otros por favor remitirse al numeral 9.1.4 Valoración del riesgo para cada uno de los activos, tabla 18.

Tabla 34.Actividades criticas del proceso

Proceso	Actividad critica	Responsable
PLANEACIÓN ESTRATÉGICA	Planeación estratégica con relación a la razón misional y visional del negocio logrando el posicionamiento del Hospital San Francisco de Gachetá.	Dirección General
EVALUACIÓN ESTRATÉGICA, ANÁLISIS Y MEJORA	Medición del desempeño del sistema de gestión integral, se pueden establecer procesos como auditorias para el cumplimiento de este ítem	Dirección General
GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN	Implementación de un sistema de gestión de seguridad informática para proteger los activos	Director del departamento de seguridad informática

	de información del Hospital Sam Francisco de Gachetá.	
GESTIÓN DE OPORTUNIDAD ES	Gestión de negocios, firmar contratos de servicios, convenios y licitaciones	Director Financiero
GESTIÓN DE LA EJECUCIÓN	Desarrollo de productos de acuerdo a lo requerido por el usuario, verificar la efectividad de satisfacción del servicio recibido.	Director general
GESTIÓN HUMANA	Efectuar contratación de personal idóneo y mantener a quien muestre los mejores rendimientos, capacitar en nuevos procesos o actualización de los mismos	Responsable de recursos humanos
GESTIÓN DE RECURSOS ADMINISTRATIVOS	Gestión de recursos físicos y económicos para el hospital. Efectuar las compras y pagos a los proveedores de la compañía. Administrar y mantener la tecnología que soporta las operaciones de la	Director financiero

	entidad. Gestionar la contabilidad de la entidad.	
GESTIÓN DOCUMENTAL	Creación, edición y distribución de los documentos necesarios para el desarrollo de los proyectos del Hospital, gestionar la correspondencia a los diferentes departamentos.	Secretarios y recepcionista

Fuente: Autor

Tabla 35. Software y herramientas.

SOFTWARE Y HERRAMIENTAS	DESCRIPCIÓN	CRITICIDAD	RESPONSABLE
Aplicaciones de tipo hospitalario con historias clínicas de los pacientes.	Aplicación destinada al almacenamiento de historias clínicas del Hospital	9	Departamento de sistemas
Bases de datos financieras	Archivo de bases de datos con información financiera del Hospital	9	Departamento de sistemas y funcionarios de administrativa
Bases de datos y documentos	Archivo de bases de datos con	9	Departamento de sistemas y

administrativos.	información administrativa del Hospital		funcionarios de administrativa
Microsoft Windows 7Professional	Sistema operativo de los puestos de trabajo	6	Departamento de sistemas
Windows server	Sistema operativo de los servidores del Hospital de trabajo	6	Departamento de sistemas
Navegadores web	Motor de búsqueda y navegación de internet.	3	Departamento de sistemas
Software de herramientas ofimáticas	Herramientas para elaboración de documentos, hojas de cálculo, presentaciones etc.	3	Departamento de sistemas
CNT programa de gestión administrativa, (programa eje del funcionamiento del hospital)	Programa de gestión administrativa del hospital.	9	Departamento de sistemas y funcionarios de Historias clínicas

Fuente: Autor

Tabla 36. Hardware y herramientas.

HARDWARE	DESCRIPCIÓN	LOCALIZACIÓN	CRITICIDAD	RESPONSABLE
34 computadores de escritorio	Puestos de trabajo de los funcionarios administrativos y de historias clínicas	Puestos de trabajo	4	Departamento de sistemas
1 servidor local	Equipo de almacenamiento de tráfico de red y copias de seguridad.	Cuarto de sistemas	6	Departamento de sistemas
Router	Recepción de internet	Cuarto de sistemas	3	Departamento de sistemas
3 Swicth	Distribución de datos en la red, permite la comunicación entre los equipos	1 en área administrativa, 1 en área financiera, 1 en historias clínicas	3	Departamento de sistemas
Planta de energía eléctrica	Soporte para mitigar fallos de la red eléctrica.	Cuarto de planta, parte trasera del Hospital	3	Departamento de sistemas, departamento de infraestructura
Cableado estructurado	Distribución de energía eléctrica a los	Según necesidades de la red en	4	Departamento de sistemas, departamento

	puestos de trabajo.	canaleta.		de infraestructura
Instalaciones eléctricas trifásicas.	Distribución de energía eléctrica en 3 fases, posibilita la conexión de equipos de alto consumo	Según necesidades de la red cableado de la infraestructura física.	4	Departamento de sistemas, departamento de infraestructura

Fuente: Autor

Análisis de riesgos

Para verificar el proceso completo de análisis de Riesgo realizado en el Hospital San Francisco de Gachetá por favor remitirse al Capítulo 9 Metodología Magerit Aplicado Al Hospital San Francisco de Gachetá.

FASE II – SELECCIÓN DE ESTRATEGIAS

En esta fase se determina las estrategias a implementar cuando se materialice una amenaza para de los activos de información del Hospital San Francisco de Gachetá a pesar de haber implementado el SGSI, la estrategia seleccionada debe garantizar una respuesta efectiva para obtener menor tiempo de restauración del activo informático.

Selección de estrategias

Existen diferentes métodos que se pueden aplicar dentro del Hospital San Francisco de Gachetá para mitigar la materialización del riesgo, cada una de estas acciones requerirá de tiempo, costos y aplicaciones de diferentes conocimientos, se debe evaluar esta serie de acciones estratégicas para que den respuesta oportuna ante incidentes dependiendo de la razón visional y misional del Hospital San Francisco de Gachetá.

Las diferentes estrategias que se implementan en el plan de contingencia de la entidad son:

- **No hacer nada:** Esta estrategia se implementará para la materialización de amenazas con una valoración de riesgo muy baja.

- **Utilización de espacios propios:** Esta estrategia se implementará cuando se requiera modificar por materialización de amenazas en espacios físicos el emplazamiento de los equipos relacionados con los puestos de trabajo de los funcionarios del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá.

- **Reutilización de recursos:** Esta estrategia se implementará cuando alguno de los activos de información Hardware y Software ha sido afectado por la materialización de una amenaza
- **Sitio alternativo subcontratado a terceros:** Esta estrategia se implementará cuando alguno de los espacios físicos del Hospital San Francisco de Gachetá es afectado por la materialización de una amenaza.

FASE III- DESARROLLO DEL PLAN

Una vez definido el análisis de la situación del Hospital San Francisco de Gachetá en lo relacionado con el análisis de riesgos se procede a establecer el plan de continuidad del negocio por lo que es necesario identificar:

- Los equipos requeridos para el desarrollo del Plan.
- Las responsabilidades y funciones de cada uno de los equipos.
- Las dependencias orgánicas entre los diferentes equipos.
- El desarrollo de los procedimientos de alerta y actuación ante eventos que puedan activar el Plan.
- Los procedimientos de actuación ante incidentes.
- La estrategia de vuelta a la normalidad.

Los equipos de emergencia estarán formados por funcionarios claves dentro del cumplimiento del proceso funciona y visional de la entidad ya que estos tendrán pleno conocimiento del proceso y las acciones correctivas para la activación del plan de continuidad del negocio.
El número de integrantes no está estandarizado, este dependerá de cómo se aborden las estrategias y de la cantidad de activos informáticos prioritarios que se deben recuperar dentro del proceso organizacional ante un incidente.

A continuación se muestran los equipos con sus funciones que forman parte del Plan de continuidad del negocio para la entidad:

Comité de crisis: Encargado de dirigir las acciones durante la contingencia y recuperación.

Los integrantes del comité de crisis se inscriben después de la implementación del SGSI por lo que en este caso al ser una propuesta se deja solo el formato para su diligenciamiento.

Tabla 37. Comité de crisis.

NOMBRE	CARGO
BLANCA RUSSI	DIRECTOR GENERAL
AMANDA CORTEZ	SUBDIRECTOR GENERAL
MANUEL AREBALO	DIRECTOR FINANCIERO
LIGIA MARTINEZ	RESPONSABLE DE RECURSOS HUMANOS
RICARDO OLAYA	DIRECTOR DEPARTAMENTO DE SEGURIDAD

Fuente: Autor

Se deben establecer lugares de encuentro previamente definidos donde se realizaran los encuentros del comité de crisis:

- Lugar de reunión 1: Sala de juntas del Hospital San Francisco de Gachetá.

- Lugar de Reunión 2: Oficina de gerencia del Hospital San Francisco de Gachetá.

Una vez un funcionario del área administrativa o de historias clínicas del hospital notifique sobre la materialización de una amenaza se procederá a activar el comité de crisis.

Se debe realizar un monitoreo de las amenazas y su posible materialización, esto se puede realizar por auditorías internas, informes del departamento de sistemas o notificaciones de los funcionarios.

Una vez materializada la amenaza y activado el comité de crisis se procederá a notificar al equipo de recuperación sobre la situación presentada para llegar a cabo si el proceso de recuperación del activo.

Equipo de recuperación: Su función es restablecer todas las funciones del activo informático en el menor tiempo posible permitiendo así tener nuevamente la recuperación de la integridad del activo informático restableciendo su disponibilidad.

Los integrantes del equipo de recuperación se inscriben después de la implementación del SGSI por lo que en este caso al ser una propuesta se deja solo el formato para su diligenciamiento.

Tabla 38. Equipo de recuperación.

EQUIPO DE RECUPERACIÓN	
Nombre	Cargo
RICARDO OLAYA	DIRECTOR DEPARTAMENTO DE SEGURIDAD
TITO PARRA	DIRECTOR DE INFRAESTRUCTURA.
MIGUEL CARDENAS	RESPONSABLE DEPARTAMENTO DE SISTEMAS
CARLOS ACERO	SOPORTE DE PRODUCTOS INSTALADOS PARA DESARROLLOS

Fuente: Autor

El equipo de recuperación es el encargado de volver a la normalidad la prestación del servicio en el Hospital San Francisco de Gachetá, su principal objetivo es eliminar la materialización de la amenaza y recuperar la funcionalidad u originalidad del activo afectado.

Para que el equipo de recuperación pueda cumplir satisfactoriamente con una respuesta efectiva debe realizar lo siguiente:

- Se deben poner en marcha los activos de información por orden de criticidad, entre más crítico sea el activo de información más rápido debe recuperar, esto mitigara la efectividad de la materialización de la amenaza hasta su corrección total

- Con relación a los activos de información se debe recurrir a la última copia de seguridad elaborada, es indispensable que el hospital cuente con un programa de copias de seguridad.

- Se debe evaluar el funcionamiento de los activos afectados y tratar de reutilizarlos, de lo contrario se debe acudir a las pólizas de seguros para hacerlas efectivas o se debe realizar la compra de los mismos con recursos del fondo de emergencias o llegar a acuerdos de pago con los proveedores en los plazos que se estimen convenientes.

- Una vez recuperados los activos se deben evaluar los controles y aumentar la exigencia de cumplimiento, si el riesgo residual es muy similar al anterior se debe cambiar el control.

Equipo logístico: Es el responsable de construir y ejecutar la logística necesaria para recuperar, reutilizar o adquirir el activo de información afectado.
En función del tipo de incidente se encargará de:

- Dar respuesta efectiva a las necesidades de logística que llegan tan pronto se detecta la materialización de la amenaza.

- Contactar con los proveedores para adquirir el material y activos necesarios que requiera el equipo de recuperación.

El listado de proveedores se realiza después de la implementación del SGSI por lo que en este caso al ser una propuesta se deja solo el formato para su diligenciamiento.

Tabla 39. Listado de proveedores.

LISTADO DE PROVEEDORES			
PROVEEDOR	DIRECCION	NOMBRE	DATOS DE CONTACTO

Fuente: Autor

Equipo de Relaciones Públicas: Su misión es la de informan a los usuarios y demás empleados acerca del incidente a través de un comunicado oficial donde se informe sobre la situación presentada y los nuevos tiempos de respuesta a las solicitudes de los usuarios, deberá ofertar soluciones tipo plan B para realizar una atención efectiva que mitigue las pérdidas ocasionadas por la materialización de la amenaza.

Desarrollo de procedimientos

Definidos los equipos y las funciones de cada uno ahora se debe proceder con las fases de operación del plan de continuidad del negocio

Fase de alerta

- **Procedimiento de notificación del desastre:** Cualquier funcionario del área administrativa o historias clínicas del Hospital San Francisco de Gachetá tiene la obligación de informar a su jefe inmediato sobre la situación presentada, el jefe inmediato debe informar al departamento de sistemas y de acuerdo al dictamen de este se informará al comité de crisis para su activación.

- **Procedimiento de ejecución del plan:** Una vez la información sea recibida se procederá a evaluar la situación en la reunión de emergencia del comité de crisis utilizando diferentes medios de comunicación en caso de que alguno de los integrantes no pueda estar presente (Skype, celular, webconference entre otras)

según el incidente el comité evaluará si activa el plan de continuidad o no, en caso de activarlo se procederá según lo señalado en el plan de contingencia, en caso contrario se remitirá al departamento de sistemas el caso para que el personal de esa área realice los procedimientos pertinentes y contactos con proveedores.

- **Procedimiento de notificación de ejecución del plan:** Activar los procedimientos para informar a los integrantes de los diferentes equipos que van a participar en el Plan de contingencia.

Fase de transición

- **Procedimiento de concentración y traslado de material y personas:** Una vez activado el plan de continuidad del negocio, todos los integrantes del comité de crisis deben acudir a los puntos de reunión, el departamento de sistemas debe entregar y poder a disposición todo el material previamente elaborado para la ejecución del plan B (backups, material de oficina, documentación).

- **Procedimiento de puesta en marcha del centro de recuperación:** Una vez se cuente con la disposición del material para el Plan B se debe proceder con la instalación, ejecución de procesos, o compra de equipos necesarios para iniciar la recuperación del activo de información del área administrativa o de historias clínicas del hospital San Francisco de Gachetá

Fase de recuperación

- **Procedimiento de restauración:** El proceso de restauración se realizará por el valor de criticidad de los activos informáticos en caso de que la amenaza se hubiera materializado en varios activos a la vez, esto se realizará teniendo en cuenta las tablas del ítem **determinar los procesos críticos** descrito en este

plan de contingencia en el titulo **Fase I – Análisis Del Negocio y Evaluación De Riesgos**

- **Procedimiento de soporte y gestión:** Una vez se realicen los procesos de recuperación se debe iniciar la verificación de la total funcionalidad del activo informático afectado por la materialización de la amenaza de acuerdo a las dimensiones en las que la amenaza lo hubiera afectado (confidencialidad, autenticidad, integridad, disponibilidad, trazabilidad), una vez se verifique la funcionalidad efectiva del activo informático se procede a dar por terminada la fase de recuperación.

Fase de vuelta a la normalidad

Una vez el activo sea restaurado, la amenaza hubiera sido superada y se hubiera evaluado la funcionalidad del activo de información en las dimensiones (confidencialidad, autenticidad, integridad, disponibilidad, trazabilidad), se procede a generar el proceso de vuelta a la normalidad en el Hospital San Francisco de Gachetá.

- **Análisis del impacto:** Una vez se materialice la amenaza el equipo de recuperación realizara una evaluación al activo afectado, a continuación presentará un informe al comité de crisis sobre las afectaciones y acciones a seguir con el activo informático, es decir informar si es posible restaurarlo, reutilizarlo o si por el contrario se debe adquirir uno nuevo, el comité de crisis tomará la decisión de acuerdo al informe para garantizar el normal cumplimiento visional y misional del Hospital San Francisco de Gachetá.

- **Adquisición de nuevo material:** Una vez generado el informe del equipo de restauración y evidenciando en dicho informe la necesidad de compra de equipos nuevos, el comité de crisis iniciará el proceso de adquisición haciendo efectivas las pólizas de seguros de los activos de información o la solicitud para aprobar ejecución de presupuesto del fondo de emergencia.

- **Fin de la contingencia:** Para dar finalización al plan de contingencia se debe hacer claridad en que el proceso no es inmediato, lo anterior teniendo en cuenta que la recuperación de los activos informáticos puede demorar horas, días, semanas, meses o años dependiendo del costo y los procesos que se ejecutaban con él, sin embargo se aclara que con la ejecución del plan de contingencia y las estrategias definidas se garantiza la continuidad del negocio.

FASE IV- PRUEBAS Y MANTENIMIENTO

La evaluación del plan de continuidad debe tener 2 aspectos fundamentales:

- **Realismo:** Las pruebas deben realizarse en escenarios que garanticen un realizamos del 95% y un 5% irreal, aun si es posible se debe simular un mayor porcentaje, esto disminuye la probabilidad de materialización de una nueva amenaza. (pentesting, auditorías externas, licitaciones para contratar a empresas certificadas que realicen pruebas en las diferentes dimensiones a los activos, entre otras)

- **Exposición Mínima:** Las pruebas deben programarse en horarios en los que la afectación de la atención al usuario no se vea interrumpida, para el caso del Hospital San Francisco se deben realizar las pruebas en el horario de 9:00pm a 4:00am, se debe ser cuidadoso con el proceso realizado ya que el área de historias clínicas debe estar disponible las 24 horas ya que este es vital para el proceso de la zona de urgencias por lo que se deben hacer las pruebas basándonos en estudios estadísticos que muestren los días en las que exista menor probabilidad de ingreso de pacientes a urgencias y de acuerdo a este análisis realizar las pruebas de seguridad.

Tiempos de recuperación. Según lo indicado en la Norma ISO/IEC 27001 Sistema de gestión de Seguridad de la Información se debe evaluar el plan de continuidad del negocio de acuerdo a los tiempos de respuestas efectivas para la recuperación de activos informáticos, por lo que se proponen los siguientes pasos:

- Determinar los procesos para ejecutar la simulación de la evaluación del plan de continuidad.
- Establecer los tiempos de respuesta que deben ser los más reducidos para:
  a. Reunión y localización del Comité de Crisis.
  b. Compra de hardware según la decisión del comité de crisis previo informe del equipo de recuperación (servidores, estaciones de trabajo)
  c. Compra de software según la decisión del comité de crisis previo informe del equipo de recuperación
  d. Instalación de copias de seguridad
  e. Restauración del sistema en los puestos de trabajo afectados del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá
  f. Determinar canales de comunicación.
  g. Reanudar actividades y procesos.
  h. Análisis de los resultados de los tiempos de ejecución reales.
  i. Realizar mejoras al plan de continuidad de negocio de acuerdo a los resultados obtenidos.

- **Pruebas plan de continuidad del negocio.** Como parte del desarrollo del plan de continuidad del negocio, es necesario determinar las actividades que permitan comprobar la eficacia del plan sin que estas afecten las actividades normales de operación de la organización y poder tomar acciones que permitan mejorar el plan de continuidad del negocio.

Tabla 40. Plan de pruebas de continuidad del negocio.

ACTIVIDAD	PARTICIPANTES	FECHA
Prueba de Escritorio	• Gerencia • Departamento de sistemas	Primer semestre del 2016
Aceptación de riesgos plan de continuidad de negocio	Gerencia Departamento de sistemas.	Primer semestre del 2016

Fuente: Autor

12. IMPACTO Y RESULTADOS

Tras realizar el diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital san francisco de Gachetá se han obtenido los siguientes resultados:

- Se requiere de una implementación del SGSI ya que tras el análisis de valoración del riesgo se evidencia la existencia de amenazas que afectan directamente el cumplimiento de los objetivos misionales y visionales de la entidad.
- Según el análisis de las amenazas a las que está expuesta la información del Hospital San Francisco de Gachetá, es fundamental considerar que la propuesta del diseño elaborada en este proyecto sea implementada según lo expuesto para mitigar riesgo de materialización de una amenaza.
- Desde recursos humanos y gerencia se deben establecer acuerdos de confidencialidad en especial a los funcionarios del área administrativa y de historias clínicas previa capacitación en seguridad informática a dichos funcionarios.
- Se evidenció la necesidad de crear el plan de copias de seguridad con menores tiempos, ya que si se realiza solo una copia de seguridad semanal se corre el riesgo de perder activos de información en gran cantidad lo que afecta la integridad y disponibilidad de la información.
- Se evidencia la necesidad de crear un plan de asignación de contraseñar y generar caducidad de las mismas en cada uno de los usuarios, lo anterior mejorará la confidencialidad, integridad y autenticidad de la información.
- Es necesario que el Hospital San Francisco de Gachetá exija a sus funcionarios del departamento de sistemas conocimientos avanzados en seguridad informática, se sugiere generar un convenio académico con la UNAD para que estos funcionarios realicen la ingeniería de sistemas para quienes sean tecnólogos o especialización en seguridad informática para

quienes sean ingenieros.

- Se deben crear procedimientos seguros para el ingreso al área administrativa y de historias clínicas, se sugiere la instalación de dispositivos biométricos para la verificación y registro de los funcionarios del área.
- Se evidencia la necesidad de establecer planes de mantenimiento preventivo y correctivo en menores tiempos ya que de no realizarse el proceso de mantenimiento preventivo se pone en riesgos los activos de información por agotamiento de recursos afectando las diferentes dimensiones de los mismos.
- El departamento de sistemas debe mejorar los procesos para la restricción de instalación de software y hardware ya que se evidencia instalación de programas que no corresponder al cumplimiento misional y visional de la entidad, se deben implementar las políticas propuestas en este documento.

13. RECOMENDACIONES

Las recomendaciones realizadas son:

- Según el análisis de las amenazas a las que está expuesta la información del Hospital San Francisco de Gachetá, se hace necesario implementar la propuesta del diseño elaborada en este proyecto para mitigar riesgo de materialización de una amenaza.
- Se debe generar un proceso de actualización de inventario de acuerdo a una periodicidad más estricta y de esta manera mitigar el desconocimiento de perdida de algún activo informático y dentro de este detallar información sobre su estado actual donde se aclare si el activo está funcionando, ha sido reparado entre otros.
- Se debe crear el plan de copias de seguridad con menores tiempos, ya que si se realiza solo una copia de seguridad semanal se corre el riesgo de perder activos de información en gran cantidad.
- Se hace necesario crear un plan de asignación de contraseñar y generar caducidad de las mismas en cada uno de los usuarios, lo anterior mejorará la confidencialidad, integridad y autenticidad de la información.
- Es necesario que el Hospital San Francisco de Gachetá exija a sus funcionarios del departamento de sistemas conocimientos avanzados en seguridad informática, se sugiere generar un convenio académico con la UNAD para que estos funcionarios realicen la especialización en seguridad informática.

14. CRONOGRAMA DE ACTIVIDADES

ACTIVIDADES	MES1				MES2				MES3				MES4			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Realizar visita de reconocimiento de la red para identificar los activos informáticos.																
Entrevistar al o los encargados del soporte de la red informática.																
Realización de encuestas sobre conocimientos básicos en seguridad informática al 20% de los usuarios.																
Implementación de la metodología MAGERIT en la entidad hospitalaria.																
Seleccionar los dominios de acuerdo a la normal que sean pertinentes y que respondan a las necesidades de seguridad de la entidad hospitalaria.																
Seleccionar los parámetros y políticas a implementar de acuerdo a la normal que sean pertinentes y que respondan a las necesidades de seguridad de la entidad hospitalaria.																
Diseño de SGSI para la entidad según las necesidades, vulnerabilidades y amenazas detectadas.																
Elaboración de propuesta final para mantener la integridad, confiabilidad y disponibilidad de la información.																

15. CONCLUSIONES

- El diseño de un sistema de gestión 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 el normal funcionamiento del Hospital.

- Al establecer políticas de seguridad informática para el hospital San Francisco de Gacheta a través del diseño de un sistema de gestión de seguridad de la información SGSI basado en la norma ISO/IEC 27001-27002 versión 2013 para mejorar el nivel de confiabilidad en el área administrativa y de historias clínicas del hospital San Francisco de Gachetá se puede concluir que los procesos de seguridad establecidos previos al desarrollo del proyecto eran mínimos ya que muchos de los equipos donde se almacena la información y su acceso a ella no contaba con protocolos de autenticación para los usuarios por lo que cualquier persona podía tener acceso a ella poniendo en riesgo su autenticidad, confiabilidad, integridad y disponibilidad. Con el diseño del SGSI se propone al Hospital proceder con su implementación para hacer más seguros sus procesos informáticos en el área administrativa y de historias clínicas.

- Al determinar los activos informáticos con autorización de la entidad hospitalaria para elegir los dominios de la norma ISO/IEC 27001-27002 versión 2013 y aplicarlos en la evaluación de riesgos se determinó que existen serios problemas en el control de acceso a la información y en la confidencialidad de la misma, por otro lado se hace necesario implementar procesos de seguridad para las operaciones en cuanto a procedimientos y responsabilidades del personal técnico y funcionarios del área administrativa e historias clínicas debido a que no se ha puesto

en marcha un proceso serio para el control del malware, virus y demás vulnerabilidades técnicas por lo que es fundamental proceder con la implementación del SGSI en el Hospital San Francisco de Gachetá.

- Al analizar las posibles vulnerabilidades y amenazas informáticas a las que se ve expuesta información digital del Hospital San Francisco de Gachetá tras aplicar la metodología MAGERIT se encontró que existen amenazas de tipo errores y fallos no intencionados que se basan en errores de usuarios, administrativos o de configuración, lo anterior conlleva a la materialización de la degradación de la información, fugas de información, difusión de software dañino y divulgación de la información siendo esta ultima la más recurrente dentro del personal administrativo. Con MAGERIT se identificó también que acciones como la manipulación de la configuración, el abuso de los privilegios de acceso y acceso no autorizado son recurrentes por parte de los funcionarios del hospital por lo que es necesario implementar las políticas de seguridad diseñadas en el presente documento.

- Al determinar los parámetros y las políticas que se deben implementar en un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001-27002 versión 2013 en el Hospital San Francisco de Gachetá se propone en primer lugar establecer políticas de seguridad de la información para mantener un control de inventarios de activos informáticos, este debe responder a una necesidad que justifique la adquisición e instalación de un los mismos haciendo responsable al funcionario usuario quien estará dotado de una contraseña de acceso, en segundo lugar se debe capacitar al personal en seguridad informática, dicho personal debe cumplir obligatoriamente con la capacitación en su totalidad, en tercer lugar se debe crear un compromiso de confidencialidad de la información entre el hospital y funcionarios del área administrativa y de historias clínicas, el desacato de dicho acuerdo tendrá sanciones legales, en cuarto lugar se debe garantizar el cubrimiento de requisitos mínimos para el funcionamiento

de la red, dichos requisitos se basan en el fluido eléctrico, infraestructura en buenas condiciones, correcto funcionamiento de los activos informáticos, caracterización del perfiles y verificación de antecedentes del personal contratado y a contratar, finalmente se debe garantizar la seguridad física de los equipos a través del control acceso, pólizas, seguros y mantenimiento preventivo de la infraestructura.

- El diseño del SGSI de acuerdo a los resultados obtenidos en los análisis de vulnerabilidades y amenazas teniendo en cuenta los controles de la norma ISO/IEC 27001-27002 versión 2013 para el área administrativa y de historias clínicas del hospital San Francisco de Gachetá ha tenido como resultado un SGSI el cual debe implementarse en 4 fases, en la primera conocida como planificar se realiza un análisis diferencial y de riesgos donde se revisa la pertinencia de los controles ISO propuestos y se expone el estado actual de los mismos, cada uno con sus observaciones, en la fase 2 se propone aplicar los controles, realizar la sensibilización y capacitación al personal de las áreas afectadas donde se implementaran los programas de gestión de incidentes y gestión de recursos, en la fase 3 se realizará la verificación y seguimiento al SGSI a través de un monitoreo el cual debe responder a un cronograma complementado con auditorías internas y externas para finalizar con el mantenimiento y mejora del sistema cuyo único objetivo siempre será la mitigación de la materialización del riesgo en cualquiera de sus dimensiones y que en caso de materializarse se contendrá con el plan de continuidad del negocio expuesto en el presente documento.

- Las medidas y controles que se proponen en este documento deben pasar a un análisis de implementación, lo anterior debido a que se requiere de una inversión de capital para garantizar la ejecución del mismo.

- Utilizando la Metodología MAGERIT 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 ve afectado.

- Las políticas nombradas en este documento deben implementarse en el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá y son los funcionarios de las diferentes áreas involucradas en el proceso los primeros responsables de su cumplimiento, por otro lado es importante que desde la gerencia y el departamento de sistemas se realice un monitoreo constante al cumplimiento del proceso, de no ser así su incumplimiento por cualquiera de las partes constituye una nueva amenaza para la protección de los activos de información.

- Uno de los aspectos que sobresalen en el desarrollo de las políticas de seguridad propuestas en el sistema de gestión de seguridad informática para el Hospital San Francisco de Gachetá, hace referencia al análisis legal con respecto a la normatividad de delitos informáticos, estableciendo de esta forma las restricciones y posibles sanciones al personal del área administrativa y de historias clínicas de la entidad hospitalaria, haciéndolo un proceso asertivo, específico, claro y consciente.

- Es muy importante recomendar que los procesos de control realizados al Sistema de Gestión de Seguridad Informática del hospital sean supervisados por personal idóneo, ya que se requiere que el funcionario encargado verifique el cumplimiento de estándares en seguridad informática, tenga conocimiento de normatividad legal vigente, conozca cómo realizar ataques informáticos a sistemas operativos y bases de datos para que así pueda saber cómo repelerlos y establecer controles oportunos ante las diferentes amenazas que se presenten en la red.

- Los controles establecidos por la norma ISO/IEC 27001- 27002 versión 2013 para el área administrativa y de historias clínicas del Hospital San

Francisco de Gachetá deben ser revisados oportunamente, según los cronogramas establecidos en el diseño del SGSI, ya que estos pueden considerarse obsoletos o insuficientes debido a que las características de las amenazas son cambiantes en el tiempo, incluso las amenazas existentes actualmente pueden aumentar su nivel de riesgo haciendo ineficientes las políticas de seguridad establecidas.

BIBLIOGRAFÍA

COMPUTER FORENSIC. Definición de delito informático. [Consultado 22 de Septiembre de 2015]. Disponible en Internet:http://www.delitosinformaticos.info/delitos_informaticos/definicion.html

EL PORTAL DE ISO EN ESPAÑOL. ISO 27000. [Consultado 18 de octubre de 2015]. Disponible en Internet: Es http://www.iso27000.es/sgsi.html

GCFA APRENDE LIBRE. ¿Qué es un virus informático? [Consultado 28 de Septiembre de 2015]. Disponible en Internet: http://www.gcfaprendelibre.org/tecnologia/curso/virus_informaticos_y_antivirus/los_virus_informaticos/1.do

INFORMATICA HOY. Seguridad informática. Todo sobre las Contraseñas. [Consultado 10 de Septiembre de 2015]. Disponible en Internet: http://www.informatica-hoy.com.ar/software-seguridad-virus-antivirus/Contrasenas-Seguridad-informatica.php.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN (ICONTEC). Norma Técnica NTC-ISO/IEC Colombiana 27001. [Consultado 18 de octubre de 2015]. Disponible en Internet: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

KASPERSKY LAB. ¿Qué es un código malicioso? [Consultado 13 de Septiembre de 2015]. Disponible en Internet:http://latam.kaspersky.com/mx/internet-security-center/definitions/malicious-code.

LA PROFESIÓN DE ADMINISTRADOR INFORMÁTICO. Administrador informático. [Consultado 10 de Septiembre de 2015]. Disponible en Internet: http://www.educaweb.com/profesion/administrador-informatico-55/. leccin_19_anlisis_de_requisitos_y_diseo_del_sgsi.html.

MINISTERIO DE EDUCACIÓN CULTURA Y DEPORTE DE ESPAÑA. Vulnerabilidades de un sistema informático. [Consultado 28 de Septiembre de 2015]. Disponible en Internet: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3

MINISTERIO DE TELECOMUNICACIONES DE COLOMBIA. Ley 1273 de 2009 de la protección de la información y de los datos. [Consultado 28 de Septiembre de 2015]. Disponible en Internet: www.mintic.gov.co/portal/604/articles-3705_documento.pdf

PANDA SEGURITY. Gusanos Informáticos. [Consultado 24 de Septiembre de 2015]. Disponible en Internet:http://www.pandasecurity.com/colombia/homeusers/security-info/classic-malware/worm/

PORTAL ADMINISTRACIÓN ELECTRÓNICA. Metodología Margerit. [Consultado 18 de octubre de 2015]. Disponible en Internet: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.ViL1eH4vfIU

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD Escuela de Ciencias Básicas, Tecnología e Ingeniería Modulo Curso: Sistema de Gestión de la Seguridad de la información SGSI.

UNIVERSIDAD NACIONAL ABIERTA YA DISTANCIA UNAD. Análisis de requisitos y diseño del SGSI. [Consultado 18 de octubre de 2015]. Disponible en Internet: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003online/44_

UNIVERSIDAD NACIONAL DE COLOMBIA. Recursos requeridos para el desarrollo del proyecto. [Consultado 28 de Septiembre de 2015]. Disponible en Internet:http://www.virtual.unal.edu.co/cursos/agronomia/2007841/lecciones/03_07.htm

UNIVERSIDAD NACIONAL DE LUJÁN. Amenazas a la Seguridad de la Información. [Consultado 10 de Septiembre de 2015]. Disponible en Internet: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12.

ANEXOS

Anexo A Solicitud Tramitada ante el Hospital

Gachetá - Febrero 24 de 2016

Doctora:

BLANCA ENEIDA RUSSI QUIROGA

Gerente Hospital San Francisco De Gachetá.

En primer lugar deseándole éxitos en sus labores profesionales.

En segundo lugar solicito su valiosa colaboración para que se me autorice realizar un inventario de los activos informáticos relacionados con trámites adminitrativo-financieros y de historial clínico de los paciente a cargo de su importante entidad.

La anterior solicito se realiza ya que en mi calidad de estudiante de especialización en seguridad informática de la Universidad Nacional Abierta y a Distancia he tomado al Hospital San Francisco de Gachetá para elaborar el proyecto **"DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMATICA BASADO EN LA NORMA ISO/IEC 27001- 27002 PARA EL AREA ADMINISTRATIVA Y DE HISTORIAS CLINICAS DEL HOSPITAL SAN FRANCISCO DE GACHETÁ"** y se requiere de dicha información para iniciar el desarrollo del mismo lo cual no afectara la información ni el funcionamiento del proceso hospitalario.

De antemano agradezco su valiosa Colaboración

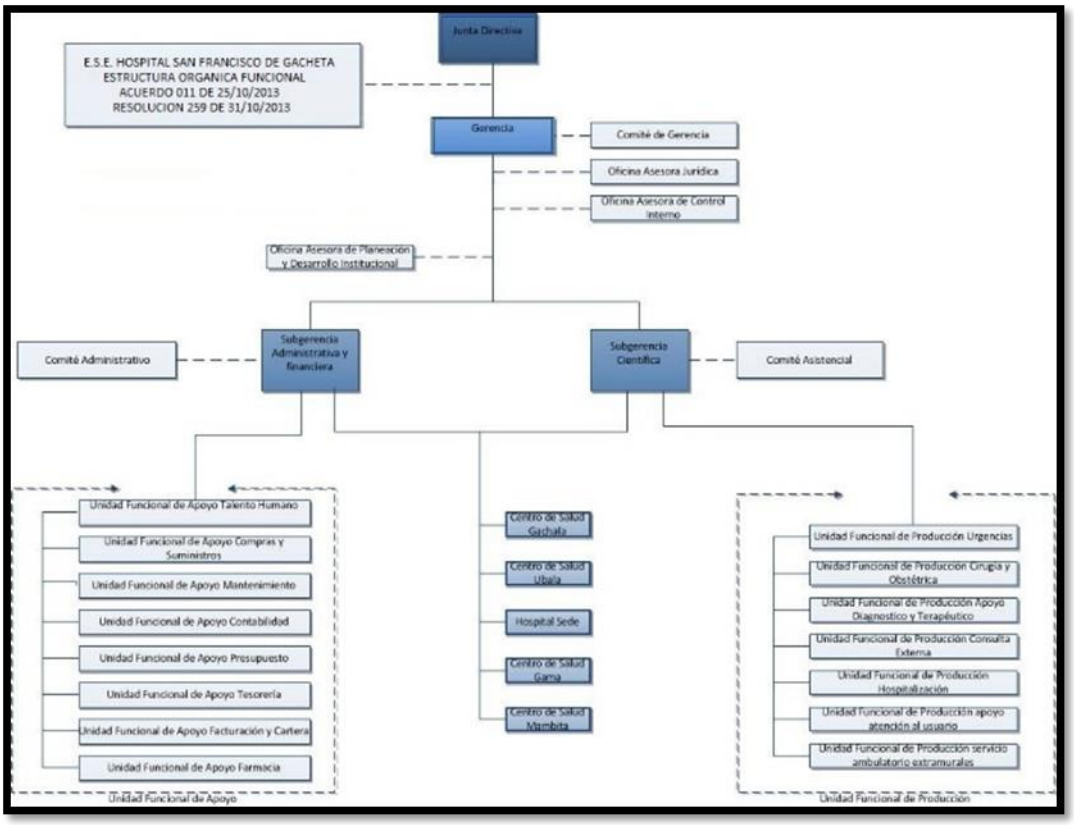
Atentamente:

Ing. Edgar Alonso Bojacá Garavito

Estudiante especialización Universidad Nacional Abierta y a Distancia.

ANEXO C. Organigrama general del Hospital San Francisco de Gachetá

Figura 3 Organizagrama hospital



FUENTE: Hospital San Francisco de Gacheta. Manual de procedimientos E.S.E Hospital San Francisco de Gachetá

ANEXO D. Organigrama general del departamento de sistemas Hospital San Francisco de Gachetá

Figura 4 Organigrama General del departamento de sistemas Hospital San Francisco de Gachetá

FUENTE: Hospital San Francisco de Gacheta. Manual de procedimientos E.S.E Hospital San Francisco de Gachetá

ANEXO E. Organigrama control interno del Hospital San Francisco de Gachetá

Figura 5. Organigrama control interno del Hospital San Francisco de Gachetá

FUENTE: Hospital San Francisco de Gacheta. Manual de procedimientos E.S.E Hospital San Francisco de Gachetá

ANEXO F. Perfiles del departamento de sistemas

PERFILES DEL DEPARTAMENTO DE SISTEMAS

Cargo: Jefe de Sistemas
Sexo: Femenino o Masculino
Edad: Mínimo 30 años

Parámetros	Requisitos
Formación Académica	Titulo especialista en seguridad informática o en proceso de formación.
	Título profesional de Ingeniero en Sistemas
	Título en carreras afines acreditado
Experiencia Laboral	Más de 3 años de experiencia en el cargo o en posiciones similares
Habilidades	Excelentes relaciones personales y facilidad para relacionarse
	Capacidad de planificación
	Capacidad para trabajar bajo presión
	Liderazgo para conducir al personal a su cargo

Tabla Perfil de Cargo Jefe de Sistema

Libertad y Orden	EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN FRANCISCO DE GACHETA	Código: MC-MJ-FOR-001-V1	Página 196 de 211
		Fecha vigencia:	HOSPITAL SAN FRANCISCO II NIVEL DE ATENCION - EMPRESA SOCIAL DEL ESTADO GACHETA - CUNDINAMARCA
		Documento Controlado	

Cargo: Asistente de Sistemas / Desarrollador
Sexo: Femenino o Masculino
Edad: Mínimo 20 años

Parámetros	Requisitos
Formación Académica	Estudiante en la carrera de Ingeniería en Sistemas
	Estudiante universitario en carreras afines
Experiencia Laboral	Más de 1 años de experiencia en el cargo o en posiciones similares
Habilidades	Excelentes relaciones personales
	Capacidad para ejecutar directrices
	Capacidad para trabajar bajo presión
	Iniciativa para el cumplimiento de tareas encomendadas

Tabla Perfil de Cargo Asistente de Sistemas / Desarrollador

ANEXO G. Registro de inconformidades de aplicabilidad de políticas de seguridad

REGISTRO DE INCONFOMIDADES DE APLICABILIDAD DE POLÍTICAS DE SEGURIDAD

FECHA: _____

FUNCIONARIOS	ÁREA DE TRABAJO	INCONFORMIDAD	ACCIÓN
(Nombre de Empleado de la observación)	(Área de Trabajo del Empleado)	(Observación reflejada en el formulario aplicado)	(Capacitación o Reunión de Revisión de Políticas de Seguridad)

_____

Firma de Elaboración

Fecha de Revisión (Gerencia): _____

.

ANEXO H. Registro de asistencia de verificación de aplicabilidad de políticas de seguridad

FECHA DE VERIFICACIÓN: _____

FORMULARIO APLICADO: _____

LUGAR DE APLICACIÓN : _____

SUPERVISOR : _____

FUNCIONARIO	HORA DE ENTRADA	FIRMA	HORA DE SALIDA	FIRMA
(Nombre del empleado que realiza el formulario de verificación)	(Hora que ingresa a la verificación)	(Firma de constancia de la entrada del empleado)	(Hora que egresa a la verificación)	(Firma de constancia de la salida del empleado)

_____ _____

Firma de Supervisión *Firma de Revisión*

Fecha de Revisión: _____

ANEXO I. Carta de convocatoria a funcionarios para capacitación.

FECHA DE CREACIÓN

Nombre del funcionario
Área de Trabajo

Cordial saludo:

Por medio de la presente se le convoca a la capacitación <<NOMBRE DE LA CAPACITACIÓN>>, dictada por <<NOMBRE DEL CAPACITADOR>>, a efectuarse el día<<FECHA DE LA CAPACITACIÓN>>, a las <<HORA DE LA CAPACITACIÓN>> en las instalaciones de <<LUGAR DE LA CAPACITACIÓN>>, donde se reforzara su entrenamiento con respecto a las políticas y procedimientos de seguridad de la información aplicados en el hospital San Francisco de Gachetá.

Le recordamos que su presencia es obligatoria.

NOMBRE DEL GERENTE GENERAL

ANEXO J. Registro de asistencia a capacitación de seguridad de información

REGISTRO DE ASISTENCIA DE

Libertad y Orden	**EMPRESA SOCIAL DEL ESTADO HOSPITAL SAN FRANCISCO DE GACHETA**	Código: MC-MJ-FOR-001-V1 Fecha vigencia: Documento Controlado	Página 200 de 211 HOSPITAL SAN FRANCISCO II NIVEL DE ATENCION - EMPRESA SOCIAL DEL ESTADO GACHETA - CUNDINAMARCA

CAPACITACIÓN DE SEGURIDAD DE INFORMACIÓN

FECHA DE CAPACITACIÓN: _____
LUGAR DE CAPACITACIÓN: _____
CAPACITADOR : _____
TEMA : _____

FUNCIONARIO	HORA DE INGRESO	FIRMA	HORA DE SALIDA	FIRMA
(Nombre del empleado que se está capacitando)	(Hora que ingresa a la capacitación)	(Firma de constancia de la entrada del empleado)	(Hora que egresa a la capacitación)	(Firma de constancia de la salida del empleado)

_____ _____
Firma de Supervisión *Firma de Revisión*

Fecha de Revisión: _____

ANEXO K. Formulario de registro de infracciones o violaciones de políticas de seguridad

ELABORADO POR: _____

FECHA	FUNCIONARIO	ÁREA DE TRABAJO	INFRACCIÓN	SITUACIÓN	ACCIÓN
(Fecha de realiza la infracción)	(Nombre de Empleado que comete la infracción)	(Área de Trabajo del Empleado)	(Infracción incurrida)	(Detalle de la situación de la infracción)	(Procedimiento Disciplinario a aplicar por motivo de la infracción)

_____

Firma de Elaboración

Fecha de Revisión (Gerencia):

_____

ANEXO L. Formulario de seguimiento de procedimientos disciplinarios

SUPERVISADO POR: _____

FECHA	FUNCIONARIOS	ÁREA DE TRABAJO	APLICADO POR:	ACCIÓN DE SEGUIMIENTO
(Fecha de seguimiento)	(Nombre de Empleado que comete la infracción)	(Área de Trabajo del Empleado)	(Persona que aplica el procedimiento disciplinario)	(Situaciones que permiten aplicar el procedimiento disciplinario)

_____

Firma de Elaboración

Fecha de Revisión (Gerencia): _____

ANEXO M. Plan de verificación de aplicabilidad de políticas de seguridad

PLAN DE VERIFICACIÓN DE APLICABILIDAD DE POLÍTICAS DE SEGURIDAD

FECHA DE PLANIFICACIÓN: _____
PERÍODO : _____

FECHA DE APLICACIÓN	ÁREA DE TRABAJO	CAUSA DE LA APLICACIÓN	FORMULARIO A APLICAR	LUGAR DE APLICACIÓN	SUPERVISOR	JUSTIFICACIÓN DE INCUMPLIMIENTO	OBSERVACIONES
(Fecha planeada para aplicación de verificación de aplicabilidad)	(Área planeada para la fecha)	(Razón de la aplicación planeada)	(Formulario a Implementar)	(Lugar de aplicación de la verificación)	(Nombre del Jefe que supervisara la aplicación de la verificación)	(Razones de incumplimiento de la verificación planificada)	(Posibles notas agregadas a la verificación planeada)

_____ _____

Firma de Elaboración ***Firma de Aprobación***

Fecha de Aprobación: _____

ANEXO N. Plan de capacitación de seguridad de la información

PLAN DE CAPACITACIÓN DE SEGURIDAD DE LA INFORMACIÓN

FECHA DE PLANIFICACIÓN: _____
PERÍODO : _____

FECHA DE APLICACIÓN	ÁREA DE TRABAJO	CAUSA DE LA CAPACITACIÓN	TEMA A TRANSMITIR	NÚMERO DE HORAS	LUGAR DE LA CAPACITACIÓN	CAPACITADOR	JUSTIFICACIÓN DE INCUMPLIMIENTO	OBSERVACIONES
(Fecha planeada para la capacitación)	(Área planeada para la fecha)	(Razón de la capacitación planeada)	(Tema de la capacitación)	(Total de horas de duración de la capacitación planeada)	(Lugar de la capacitación)	(Nombre del Jefe que supervisara la aplicación de la verificación)	(Razones de incumplimiento de la verificación planificada)	(Posibles notas agregadas a la verificación planeada)

_____ _____

Firma de Elaboración ***Firma de Aprobación***

Fecha de Aprobación: _____

ANEXO O. RESUMEN ANÁLITICO RAE.

Título de Documento.	DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD INFORMATICA BASADO EN LA NORMA ISO/IEC 27001-27002 PARA EL AREA ADMINISTRATIVA Y DE HISTORIAS CLINICAS DEL HOSPITAL SAN FRANCISCO DE GACHETÁ
Autor	BOJACA GARAVITO Edgar Alonso.
Palabras Claves	Sistema de gestión de seguridad informática, usuarios, activos informáticos, ISO/IEC 27001- 27002, Hospital San Francisco de Gachetá, integridad, disponibilidad, confidencialidad, trazabilidad, autenticidad, Metodología Magerit, funcionarios,
Descripción El proyecto Diseño de un Sistema de Gestión de Seguridad Informática basado en la norma ISO/IEC 27001- 27002 para el área administrativa y de historias clínicas del Hospital San Francisco de Gachetá es una investigación donde se analizan las vulnerabilidades y amenazas para los activos informáticos de la entidad pública en mención y como finalidad tiene garantizar la protección de estos en cada una de sus dimensiones garantizando así el buen cumplimiento de atención a pacientes de la región de Guavio.	
Fuentes Bibliográficas	COMPUTER FORENSIC. Definición de delito informático. [Consultado 22 de Septiembre de 2015]. Disponible en Internet:http://www.delitosinformaticos.info/delitos_informaticos/definicion.html MINISTERIO DE EDUCACIÓN CULTURA Y DEPORTE DE ESPAÑA. Vulnerabilidades de un sistema informático. [Consultado 28 de Septiembre de 2015]. Disponible en Internet: http://recursostic.educacion.es/observatorio/web/es/component/content/article/1040-introduccion-a-la-seguridad-informatica?start=3 MINISTERIO DE TELECOMUNICACIONES DE COLOMBIA. Ley 1273 de 2009 de la protección de la información y de los datos. [Consultado 28 de Septiembre de 2015]. Disponible en Internet: www.mintic.gov.co/portal/604/articles-3705_documento.pdf PANDA SEGURITY. Gusanos Informáticos. [Consultado 24 de Septiembre de 2015]. Disponible en Internet:http://www.pandasecurity.com/colombia/homeusers/security-info/classic-malware/worm/ UNIVERSIDAD NACIONAL DE LUJÁN. Amenazas a la

	Seguridad de la Información. [Consultado 10 de Septiembre de 2015]. Disponible en Internet: http://www.seguridadinformatica.unlu.edu.ar/?q=node/12.

CONTENIDO:

Diseño de un sistema de gestión de seguridad informática basado en la norma ISO/IEC 27001-27002 versión 2013 para el área administrativa y de historias clínicas del hospital san francisco de Gachetá

- **DESCRIPCIÓN DEL PROBLEMA:**

Gracias a los avances de la tecnología el hospital San Francisco de Gachetá ha optado por digitalizar gran cantidad de información que antes se manejaba en formatos a papel los cuales son importantes para su funcionamiento y atención oportuna de pacientes, dicha información es de carácter financiero, administrativo, historial clínico de pacientes, formulas médicas, resultados de exámenes, agendas de citas, médicas entre otros.

Al ser ISO/IEC 27001-27002 versión 2013 un estándar para la seguridad de la información nos orienta o específica los requisitos necesarios para establecer, diseñar, implantar, mantener y mejorar un sistema de gestión de la seguridad de la información (SGSI) lo que lo convierte en nuestra carta de navegación para realizar el estudio y diseño de un sistema de gestión de seguridad de la información en el hospital San Francisco de Gachetá.

Teniendo en cuenta la descripción anterior se plantea la siguiente formulación:

¿Cómo el diseño de un sistema de gestión de seguridad informática SGSI basado en la norma ISO/IEC 27001-27002 versión 2013 permitirá mejorar el nivel de confiabilidad a través del establecimiento de parámetros y políticas de seguridad de la información en el área administrativa y de historias clínicas del hospital San Francisco de Gachetá?

OBJETIVO GENERAL.

Establecer parámetros y políticas de seguridad informática mediante el diseño de un sistema de gestión de seguridad de la información SGSI basado en la norma ISO/IEC 27001-27002 versión 2013 para mejorar el nivel de confiabilidad en el área administrativa y de historias clínicas del hospital San Francisco de Gachetá.

OBJETIVOS ESPECÍFICOS.

- Determinar los activos informáticos con autorización de la entidad hospitalaria para elegir los dominios de la norma ISO/IEC 27001-27002 versión 2013 que serán aplicados en la evaluación de riesgos.
- Analizar las posibles vulnerabilidades y posibles amenazas informáticas a las que se ve expuesta información digital de hospital san francisco de Gachetá

aplicando la metodología MAGERIT.

- Determinar los parámetros y las políticas que se deben implementar en un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001-27002 versión 2013 en el hospital san francisco de Gachetá.
- Diseñar el SGSI de acuerdo a los resultados obtenidos en los análisis de vulnerabilidades y amenazas teniendo en cuenta los controles de la norma ISO/IEC 27001-27002 versión 2013 para el área administrativa y de historias clínicas del hospital San Francisco de Gachetá

RESUMEN DE LO DESARROLLADO EN EL PROYECTO.

Determinación de activos informáticos
Con autorización de la gerencia del hospital se procedió a elaborar un inventario de los activos de información con que cuenta el área administrativa y de historias clínicas de la entidad "Ver tabla 4 activos informáticos".

Vulnerabilidades y amenazas
Una vez determinados los activos de información con los que cuenta la entidad dentro del área administrativa y de historias clínicas se procede a identificar las amenazas a las cuales se exponen utilizando la metodología MAGERIT "ver tabla 16 del documento original"

Posterior a esto se ha realizado la valoración del riesgo teniendo en cuenta su nivel de impacto y probabilidad de ocurrencia en cada uno de los activos informáticos, "ver tabla 16 del documento general".

Posteriormente y de acuerdo a esta valoración del riesgo se han implementado los controles ISO 27001-2002 de acuerdo a las amenazas a las que se ve expuesto cada activo informático, "ver tabla 16 del documento general".

Una vez analizadas las vulnerabilidades se establece la valoración del riesgo, esto permitirá definir la aplicación de controles ISO 27001 – 27002 los cuales tendrán un nivel de eficacia, "ver tabla 16 del documento general".

Tras la implementación de controles y aplicación de los mismos se genera una mitigación del riesgo, lo anterior significa que el riesgo no ha sido erradicado por completo por lo que se genera una valoración de riesgo residual el cual el Hospital San Francisco de Gachetá "ver tabla 16 del documento original":

Políticas de seguridad informática para el Hospital San Francisco de Gachetá
Tras realizar el análisis de riesgos activo por activo y verificando en cada uno según su clasificación y analizando los diferentes controles según la ISO 27001 – 27002 que se van a aplicar en la entidad se establecen las siguientes políticas de

seguridad (Por ser un resumen solo se enunciarán las políticas más importantes y el objetivo, los demás ítems pueden consultarse en el documento original):

- **Políticas de seguridad de la información.**

Objetivo: Asegurar los activos de la información a través de la implementación de controles de seguridad que permitan garantizar la integridad y disponibilidad de los activos de información.

- **Políticas de capacitación y concientización de seguridad de la información.**

Objetivo: Mitigar la indisponibilidad del personal ante incidentes de seguridad de la información a través de procesos de capacitación y concientización dirigidos a los funcionarios del área administrativa y de historias clínicas del Hospital San Francisco de Gachetá.

- **Políticas de confidencialidad**

Objetivo: Evitar de manera efectiva la divulgación de la información estableciendo controles y acuerdos de confidencialidad con los funcionarios del área administrativa y de historias clínicas del hospital San Francisco de Gachetá.

- **Políticas de fluido eléctrico.**

Objetivo: Garantizar el constante suministro eléctrico en las instalaciones del Hospital San Francisco de Gachetá mitigando la interrupción del servicio por cortes eléctricos.

- **Políticas de seguridad de control de accesos**

Objetivo: Asegurar un acceso controlado, físico o lógico, a los activos informáticos del Hospital San Francisco de Gachetá.

- **Políticas de seguridad física y ambiental.**

Objetivo: Garantizar la seguridad física y ambiental de los activos de información del Hospital San Francisco de Gachetá

Diseño del SGSI para el hospital San Francisco de Gachetá

Para el diseño del sistema de gestión de seguridad informática en el Hospital San Francisco de Gachetá se han establecido el desarrollo de 4 fases que permiten el correcto y pertinente cumplimiento de las políticas de seguridad para la aplicación de controles ISO 27001 27002 de acuerdo con los análisis de amenazas y valoración del riesgo mostrado anteriormente según los cuales se han establecido políticas de seguridad que respondan a la aplicación de controles ISO cumpliendo con unos objetivos por política de seguridad y de acuerdo a unas responsabilidades asignadas.

FASE 1: PLANIFICAR: ANÁLISIS DIFERENCIAL Y DE RIESGOS PARA DEFINICIÓN DEL ALCANCE Y OTRAS ACTIVIDADES DE PLANEACIÓN.
Tras el análisis realizado de amenazas y junto con su la respectiva valoración del riesgo se han establecido una serie de controles de acuerdo a la Norma ISO 27001-27002, de acuerdo a esto se han creado políticas de seguridad las cuales tienen como fin garantizar la seguridad de los activos de información del Hospital San Francisco de Gachetá en sus diferentes dimensiones, por lo anterior es necesario elaborar un análisis diferencial concretando así un informe actual de los controles propuestos para estandarizar responsabilidades para una futura implementación del diseño sistema de seguridad informática en la entidad hospitalaria.

El análisis diferencial lo encontrará en la Tabla 20: Análisis diferencial de los controles ISO 207001-27002 para el Hospital San Francisco de Gachetá del documento original.

FASE 2: HACER: PROPUESTA PARA IMPLANTAR EL DISEÑO DEL SGSI
Para poder realizar la implementación del diseño SGSI en el hospital San Francisco de Gachetá deben realizarse una serie de pasos los cuales se relacionan a continuación:

- Aplicación de los controles ISO 27001- 27002 de acuerdo a las políticas de seguridad propuesta en el diseño.
- Implementación de controles.
- Implementación de un programa de sensibilización y capacitación.
- Implementación de un programa de gestión de incidentes.
- Gestión de recursos para el SGSI.

FASE 3: VERIFICAR: SEGUIMIENTO, SUPERVISIÓN Y REVISIÓN DEL SGSI
Este proceso de verificación debe realizarse de acuerdo al cumplimiento de los controles ISO 27001-27002 que se han seleccionado para el Hospital San Francisco de Gachetá, esto debe realizarse de manera periódica y de primera mano será responsabilidad del departamento de sistemas quienes de ser necesario solicitaran a la gerencia una licitación para contratar una revisión externa de una empresa especializada y certificada en el tema.

FASE 4: ACTUAR: MANTENER Y MEJORAR EL SISTEMA
De acuerdo con las medidas tomadas y las situaciones presentadas en la fase III y teniendo en cuenta los resultados de los controles, la métrica, monitoreo, revisión y luego de implementar el SGSI en el hospital San Francisco de Gachetá se deben analizar aquellas políticas que deban reforzarse para dar solución a los incidentes presentados para replantear las políticas, procesos o establecer sanciones respectivas con el fin de cumplir en mejor nivel con la mitigación del riesgo a los que se ven enfrentados los activos informáticos del Hospital San Francisco de

Gachetá del área administrativa y de historias clínicas.

METODOLOGÍA DE DESARROLLO

Para el desarrollo satisfactorio de la propuesta es necesario realizar 4 pasos fundamentales los cuales nos llevarán al de diseño de un sistema de seguridad informática basado en la norma ISO/IEC 27001-27002 versión 2013 en el Hospital San Francisco De Gachetá, los pasos para la metodología del desarrollo son:

- Determinar los activos informáticos de la empresa para elegir los dominios de la norma ISO/IEC 27001-27002 versión 2013 que serán aplicados en la evaluación de riesgos.

- Analizar las posibles vulnerabilidades y posibles amenazas informáticas a las que se ve expuesta información digital de hospital san francisco de Gachetá aplicando la metodología MAGERIT.

- Determinar los parámetros y políticas que se deben implementar en un sistema de gestión de seguridad de la información basado en la norma ISO/IEC 27001-27002 versión 2013 en el hospital san francisco de Gachetá.

- Diseñar el SGSI de acuerdo a los resultados obtenidos en los análisis de vulnerabilidades y amenazas teniendo en cuenta los parámetros de la norma ISO/IEC 27001-27002 versión 2013 para el área administrativa y de historias clínicas del hospital San Francisco de Gachetá aplicando políticas de seguridad informática aplicables a la realidad de la organización.

Conclusiones

- El diseño de un sistema de gestión 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 el normal funcionamiento del Hospital.

- Utilizando la Metodología MAGERIT 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 ve afectado.

Recomendaciones.

Las principales recomendaciones realizadas son:

- Según el análisis de las amenazas a las que está expuesta la información del

Hospital San Francisco de Gachetá, se hace necesario implementar la propuesta del diseño elaborada en este proyecto para mitigar riesgo de materialización de una amenaza.

- Se debe crear el plan de copias de seguridad con menores tiempos, ya que si se realiza solo una copia de seguridad semanal se corre el riesgo de perder activos de información en gran cantidad.
- Es necesario que el Hospital San Francisco de Gachetá exija a sus funcionarios del departamento de sistemas conocimientos avanzados en seguridad informática, se sugiere generar un convenio académico con la UNAD para que estos funcionarios realicen la especialización en seguridad informática.