DIAGNÓSTICO Y PLANEACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA, E.S.E.

HECTOR RICARDO TRIANA ACEVEDO

Director

M Sc. ANDRES FELIPE MILLAN CIFUENTES

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA

MAESTRIA EN GESTIÓN DE TECNOLOGÍA DE INFORMACIÓN

VIRTUAL

2018

RESUMEN

TÍTULO: DIAGNÓSTICO Y PLANEACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL HOSPITAL SAN JOSÉ DE ORTEGA, TOLIMA, E.S.E.

AUTOR: HÉCTOR RICARDO TRIANA ACEVEDO

PALABRAS CLAVE: MSPI, SGSI, DIAGNÓSTICO, PLANEACIÓN, SEGURIDAD, GEL.

DESCRIPCIÓN:

La implementación de un modelo de seguridad y privacidad de la información tiene carácter obligatorio en la legislación colombiana para las Entidades del Estado, según lo establecido en el decreto 2573 de 2014, por lo cual el presente proyecto aplicado en el hospital San José de Ortega, Tolima, abarca sus dos primeras fases como son la etapa previa a la instalación del modelo, conocida como diagnóstico y su planificación, basado en el Modelo de Seguridad y Privacidad de la Información de MINTIC. (Ministerio de las Tecnología y las Comunicaciones, 2017).

Se analiza el estado actual de la entidad en cuanto al nivel de madurez del sistema de seguridad que utiliza para salvaguardar su información, para posteriormente recoger la información que permita realizar el análisis de vulnerabilidad y de riesgo que posee la Entidad. Asimismo, se establecen las políticas de seguridad de información y se asignan los recursos humanos al proceso de seguridad de la información, efectuando el inventario de activos y alineando el modelo con el sistema de gestión documental actual.

La ejecución del proyecto abarca la determinación y la identificación de los activos vitales de información que posee la Entidad, así como las amenazas y vulnerabilidades que posee actualmente. Todo esto permite que las diferentes dependencias, incluida la alta dirección tome conciencia, a través de planes de sensibilización y capacitación.

Al concluir la ejecución del proyecto se determina e identifica el actual estado de nivel de madurez del sistema de gestión de seguridad, realizando el levantamiento de información para efectuar las pruebas que permitan medir la efectividad de los controles existentes, para posteriormente establecer las políticas de seguridad de la información; la asignación de roles y responsabilidades dentro del modelo de seguridad; y la elaboración del inventario de activos, planeando la integración del Modelo con la gestión documental del Hospital, y efectuando el análisis de riegos con su respectivo tratamiento.

ABSTRACT

TITLE: DIAGNOSTIC AND PLANNING OF THE INFORMATION SECURITY AND PRIVACY MODEL AT THE SAN JOSÉ DE ORTEGA HOSPITAL, TOLIMA, E.S.E.

AUTOR: HÉCTOR RICARDO TRIANA ACEVEDO

KEYWORDS: MSPI, ISMS, DIAGNOSIS, PLANNING, SECURITY, GEL.

DESCRIPTION:

The implementation of an information security and privacy model is mandatory in Colombian legislation for the State Entities, for which the present project applied in the San José de Ortega Hospital, Tolima, will cover its first two phases, such as the stage prior to the installation of the model, known as diagnostics and its planning, based on the technology and information architecture of this country, promoted by the Ministry of Technology and Communications, MINTIC. (Ministry of Technology and Communications, 2017).

The current state of the entity is analyzed in terms of the level of maturity of the security system that it uses to safeguard its information, and then collecting the information that allows the analysis of vulnerability and risk that the Entity has. Likewise, information security policies are established, and human resources are assigned to the information security process, making the inventory of assets and aligning the model with the current document management system.

The execution of the project covers the identification and identification of the vital information assets that the Entity possesses, as well as the threats and vulnerabilities it currently has. All this allows the different agencies, including senior management to become aware, through awareness and training plans.

At the conclusion of the execution of the project, the current level of maturity of the security management system is determined and identified, carrying out the information gathering to carry out the tests that allow to measure the effectiveness of the existing controls, to later establish the security policies of the information; the assignment of roles and responsibilities within the security model; and the preparation of the inventory of assets, planning the integration of the Model with the documentary management of the Hospital, and carrying out the analysis of risks with their respective treatment.

Contenido

Lista de Figuras

Lista de Tablas

Introducción

El Hospital San José del municipio de Ortega Tolima es una empresa social del estado colombiano que presta servicios de salud de primer nivel de complejidad administrando la información de sus usuarios que por su naturaleza tiene carácter reservado. Su prioridad en gestión de información es salvaguardar los datos personales confiados para que sean solamente conocidos por los funcionarios autorizados y el usuario del servicio (confidencialidad) y que la información no sea modificada lo que podría colocar en riesgos la vida o agravar la salud de los pacientes (integridad). Asimismo, debe velar a que la información que posee en su base de datos pueda ser accedida por las diferentes áreas del hospital en el momento que se le requiera, según labor que cumplen con la debida autorización (Disponibilidad).

Las entidades del estado por mandato legal deben realizar actividades encaminadas a evitar que sus activos de información puedan ser vulnerados por las diferentes amenazas que existen en su entorno y que puedan afectar su imagen institucional, colocando en riesgo datos personales sensibles de los ciudadanos, su presupuesto, entre otros aspectos, por lo cual se hace necesario la implementación de un Modelo de Seguridad y Privacidad de la Información, MSPI, en el Hospital San José de Ortega.

El MSPI consta de cinco fases de desarrollo, Diagnóstico, Planeación, Implementación, Evaluación de Desempeño y Mejora continua. El presente trabajo se enfoca en las dos primeras etapas de Diagnóstico y Planeación del Modelo de Seguridad y Privacidad de la Empresa Social

del Estado, E.S.E., por cuanto no se había comenzado su implementación acorde con lo estipulado en la ley 1341 de 2009 reglamentada por el decreto 2573 de 2014.

Para la ejecución de las dos primeras fases del ciclo de operación del MSPI, se siguió el modelo de gestión de tecnologías de información para las entidades colombianas: IT4+, en que basa la Estrategia de Gobierno en Línea, GEL, el cual consta de cuatro componentes, TIC para los servicios, TIC para el gobierno abierto, TIC para la gestión y Seguridad y Privacidad de la Información, siendo este último el que se abarca en esta tesis.

En el presente proyecto se realiza una descripción de la Entidad del estado donde se ejecuta el diagnóstico y planeación del MSPI. La ejecución del proyecto abarcará la determinación y la identificación actual de madurez del sistema de gestión de seguridad, realizando el levantamiento de información para efectuar las pruebas que permitan medir la efectividad de los controles existentes para posteriormente establecer las políticas de seguridad de la información; asignación de roles y responsabilidades dentro del modelo de seguridad; elaborar el inventario de activos, observando su identificación, clasificación y valoración; planear la integración del Modelo con la gestión documental del Hospital; y el análisis de riegos con su respectivo tratamiento de datos personales. Todo esto permitirá que las diferentes dependencias, incluida la alta dirección tome conciencia, a través de planes de sensibilización y capacitación. (MINTIC, 2017)

1. Definición Del Problema

El hospital San José de Ortega en la actualidad no posee políticas, controles o medidas de seguridad para preservar los datos y equipos, o bien, si existen, no se ha realizado de forma correcta su implementación y su correcta comunicación (sensibilización) lo que podría originar incidentes de seguridad que afecten la confidencialidad, la disponibilidad y la integridad de la información contenidas en sus bases de datos personales, dispositivos o la que circula por la red Institucional. (Instituto Nacional de Ciberseguridad de España, 2017)

Aunque esta Entidad ha comenzado la implementación de la política de Gobierno En Línea, según su plan de acción del año 2016 y como se evidencia en actas de comité de control interno, que reposan en esa oficina, varios de los puntos a seguir solamente se han quedado plasmados en el papel y no se les ha dado el desarrollo ordenado dentro de esta Normativa, entre ellas gestionar la infraestructura tecnológica efectuando un ajuste según las necesidades existentes para sus procesos estratégicos, que permita una excelente prestación de servicios y la interoperabilidad por medios electrónicos. (Bermúdez et al., 2011)

Por cuanto no se ha realizado ningún estudio del estado actual de madurez en el Hospital no se conoce su nivel de vulnerabilidad de su información, haciéndose prioritario la realización de esta actividad previa a la redacción de su política de seguridad y demás actividades de la etapa de planificación de su Sistema de Seguridad y Privacidad de la Información, denotándose por cuanto en los archivos físicos y digitales de la oficina asesora de gestión de calidad de esta Entidad,

encargada de esta funciones, no posee en la actualidad algún plan específico sobre el tema de gobierno en línea.

Como se menciona su principal problemática es que no se conoce el estado de madurez actual del sistema de gestión de tecnología de la Entidad, que permita lograr su optimización, según necesidades, teniéndose en cuenta en todos los procesos para lograr una efectiva seguridad de la información y que posteriormente permita generar un plan de seguridad y privacidad alineado a sus objetivos estratégicos, lo cual se colige de diálogos sostenidos con el jefe de la oficina de control interno del Hospital.

Como se deja de manifiesto en el anterior párrafo, no se tiene control sobre uno de los atributos de la información, la confidencialidad, pero también se podría ver afectada la disponibilidad, por cuanto se han conocido de recientes incidentes relacionados con la ciberseguridad donde delincuentes informáticos han cifrado los datos de las historias clínicas con software malicioso (ransomware) para posteriormente pedir rescate, poniendo en peligro la salud o incluso la vida de la victima de esta actuación ilícita.

Asimismo, los delincuentes informáticos si no se toman medidas preventivas adecuadas pueden atentar inclusive contra la integridad de la información para obtener beneficios como seguros de invalidez a través de la modificación de historias clínicas o exámenes médicos, perjudicando como se ha expuesto anteriormente tanto al cliente como a la Entidad.

Como se evidencia El hospital San José de Ortega no ha iniciado el proceso trasversal y obligatorio de seguridad y privacidad de la información para su negocio, sin conocer el estado actual en que se encuentra en éste importantísimo aspecto, por lo cual es válido preguntarse… ¿Cuál es el diagnóstico actual y la mejor planeación del sistema de gestión de seguridad y privacidad de la información en el Hospital San José de Ortega, Tolima, E.S.E.?

2. Justificación

Las entidades del nivel territorial, para este caso la ESE en mención, deben cumplir con lo dispuesto en la ley 1341 de 2009 (Alcaldía de Bogotá, 2009) y reglamentada mediante los decretos 2573 de 2014 y 1078 de 2015 (Alcaldía de Bogotá, 2015)) en las cuales se expone que es de vital importancia promover condiciones de ciberseguridad en la información que posee en sus dispositivos o circulan por la red, por lo cual esta actividad transversal es obligatoria y con la ejecución del presente trabajo se inicia la alineación de las políticas de programa de Gobierno En Línea, que le permitirá cerrar la brecha que existe en la actualidad aproximándose a un eficiente Sistema de Gestión de Seguridad Institucional.

Asimismo, cualquier Empresa de carácter público y privado debe conocer el nivel de seguridad y privacidad de los datos y equipos que administra y que en especial, para este tipo de entidades, tienen requerimientos legales especiales con respecto al manejo de información de sus usuarios, por cuanto podrían estar inmersos en procesos legales debido a su inobservancia. (Consejo Técnico de la Contaduría Pública, 2017).

Por otra parte, se ha advertido de forma directa y a través de entrevistas informales sostenidas con el gerente, con la encargada de la oficina de gestión de calidad, con el jefe de la oficina de control interno, con el encargado de la oficina de gestión de la información, con el coordinador de la sección de urgencias y con el coordinador de la sección de promoción y prevención, que en esta Entidad no existe una política instituida para salvaguardar los datos que poseen sus diferentes dispositivos y sistemas de información.

Para lograr los objetivos trazados es de vital importancia contar con el apoyo de la Gerencia y hacer partícipes a todas las dependencias del Hospital, sin diferenciar su pertenencia al proceso misional o de apoyo por cuanto cualquier persona o equipo puede ser vulnerado por las diferentes técnicas que utilizan los cibercriminales para conocer, alterar o borrar la información, o bien indisponer los sistemas de información.

Por lo antes expuesto, se hace necesario efectuar un estudio del estado de madurez de la infraestructura actual y su ajuste que permita una correcta implementación del Modelo de Seguridad y Privacidad de la Información, el cual tiene carácter obligatorio para todas las entidades públicas del ámbito nacional y territorial.

Por otra parte, con la ejecución de este trabajo de grado se consolidarán los conocimientos adquiridos dentro del pensum de la Maestría, especialmente en la Gestión de seguridad, proyectos e infraestructura, como también en la arquitectura de TI y de la Solución, que permitirán el enriquecimiento profesional del candidato a magister que la efectúa.

3. Objetivos

3.1 General

Realizar el diagnóstico y planeación del modelo de gestión de seguridad y privacidad de la información en el Hospital San José de Ortega, Tolima, E.S.E.

3.2 Específicos

- Determinar el estado actual de la gestión de seguridad y privacidad de la información en el Hospital de Ortega.
- Identificar lo que comprenden por seguridad y privacidad de la información los trabajadores de la Entidad.
- Identificar las amenazas y vulnerabilidades de los activos de información en el Hospital de Ortega.
- Establecer la Política de seguridad de la información con objetivos y alcance.
- Proponer los postulados para la redacción de los procedimientos de seguridad de la información en el Hospital San José de Ortega.
- Coadyuvar a la definición roles y responsabilidades de seguridad y privacidad de la información. en la Entidad.
- Redactar la metodología para la realización de inventario de activos de información
- Planificar la Identificación, Valoración y tratamiento de datos de riesgo en el hospital San José de Ortega.

4. Marco Referencial

4.1 Marco Contextual

Hacia mediados de la década de los cincuenta en el siglo XX, fue creada la institución denominada "HOSPITAL SAN JOSE DE ORTEGA", destinado a prestar los servicios de salud de la comunidad del municipio, en el predio donado por el Doctor Nicolás Ramírez, ubicado en la calle del Cementerio con la carrera Bolívar. Posteriormente, el Concejo Municipal, mediante Acuerdo No. 017 de 1992, acuerda la creación del HOSPITAL SAN JOSE DE ORTEGA, como establecimiento descentralizado de la administración municipal. En la figura 1 se observa la entrada a urgencias de esta empresa social del estado:

Figura 1. Hospital San José de Ortega, Entrada Urgencias.

Con el advenimiento de la Ley 100 de 1993 y la Ley 489 de 1998 fue transformado en Empresa Social del Estado, por Acuerdo No. 003 de 1996 del Concejo Municipal de Ortega Tolima, denominándose HOSPITAL SAN JOSE EMPRESA SOCIAL DEL ESTADO DEL MUNICIPIO DE ORTEGA, reconociéndosele personería mediante Resolución No. 001 de noviembre de 1997 por parte de la Secretaría de Gobierno Municipal de Ortega, con el fin de prestar servicios de salud entendidos como un servicio público a cargo del Estado y parte integrante del sistema de seguridad social, en el nivel I de atención. Se observa en la figura 2 la entrada del área administrativa:

Figura 2. Hospital San José de Ortega, Entrada Oficinas Administrativas.

La población objetivo de los servicios del hospital se encuentra dentro del municipio de Ortega, población ubicada al sur del departamento, a 103 Km aproximadamente de distancia de la ciudad

de Ibagué; la cobertura de servicios llega a unos 33.873 usuarios que habitan el municipio, de los cuales el 21.88% se encuentra en la cabecera municipal y el 78.12% en 122 veredas de la zona rural. Se observa en la figura 3 la ubicación geográfica apoyado en la herramienta Google maps:

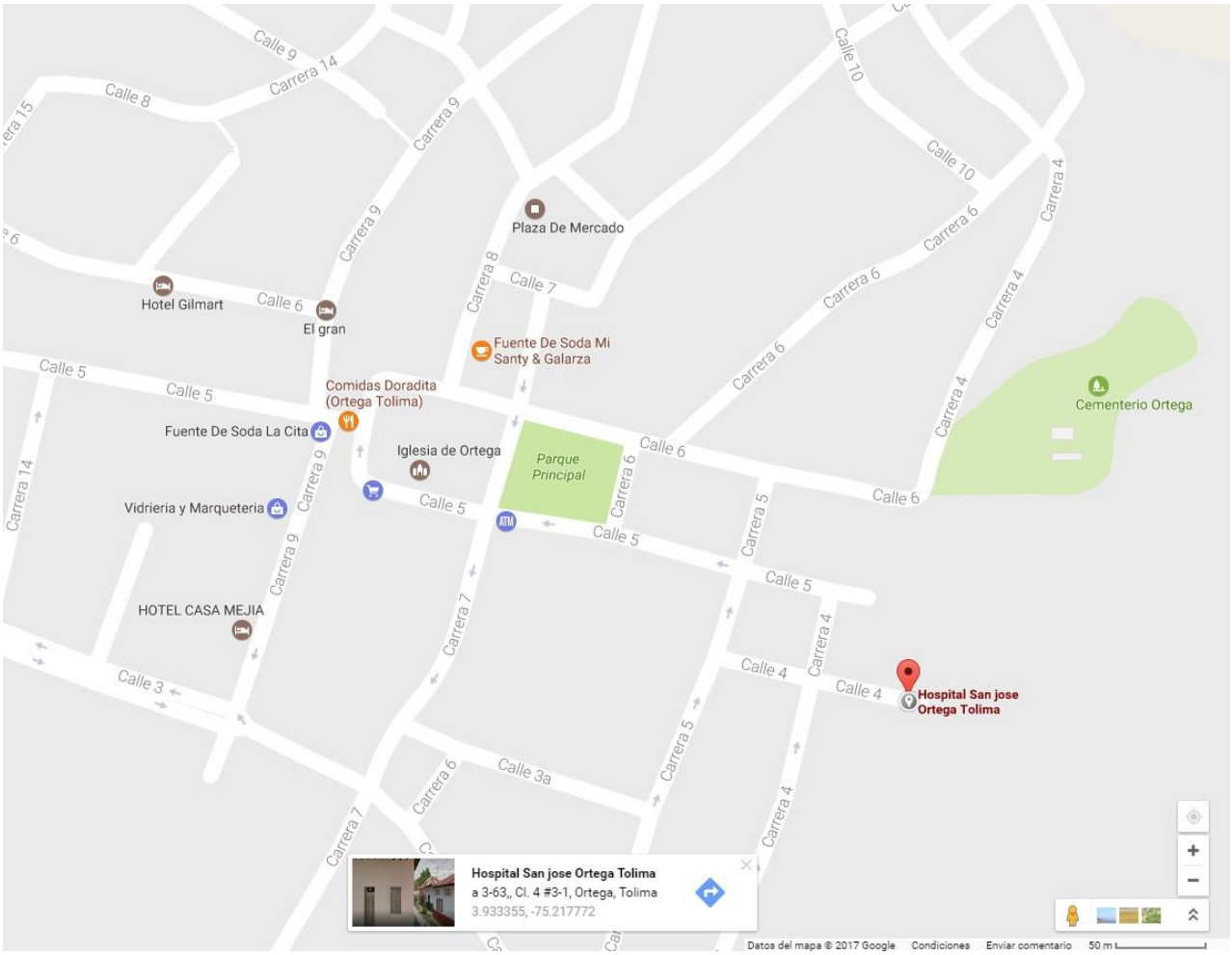


Figura 3. Hospital San José de Ortega, Ubicación Georeferencial.
Adaptado de Google Maps (2017). Tomado de: https://www.google.es/maps/place/Ortega,+Tolima/@3.9323688,-75.398949,11z/data=!3m1!4b1!4m5!3m4!1s0x8e393898ada7e24f:0x7882651ac047f9cc!8m2!3d3.935841!4d-75.220606

MISION: Somos una Empresa Social de Estado que presta servicios de primer nivel de atención, a la comunidad orteguna, comprometidos en ser solidarios, transparentes, responsables y

respetuosos. Teniendo como objetivo el bienestar integral del paciente, buscamos la excelencia en todas nuestras actividades mediante el desarrollo de las capacidades humanas, técnicas y el trabajo en equipo, ofreciendo seguridad al paciente y utilizando eficientemente los recursos.

VISION: En el año 2017 vemos a la Empresa Social del Estado Hospital San José de Ortega, como una institución modelo en la prestación de servicios de salud de primer nivel, en donde su componente técnico y humano, serán factor importante de su excelente servicio, el cual permitirá la consolidación económica de la empresa, dentro de la red de prestadores del sector.

PRINCIPIOS CORPORATIVOS:

- Compromiso
- Responsabilidad
- Disciplina
- Calidad
- Respeto
- Ética
- Solidaridad

4.2 Marco Teórico

La teoría en que se enmarca el trabajo es la norma ISO/IEC 27001 que es 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 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2. Por consiguiente, se expone los principales conceptos relacionados con esta norma.

4.2.1 Seguridad de la Información

La Seguridad de la Información, según ISO 27001, se refiere a la confidencialidad, la integridad y la disponibilidad de la información importante para la organización, independientemente del formato que tengan estos pueden ser: electrónicos, en papel, audio y vídeo, etc.

También se puede definir que el objetivo de la seguridad de la información es asegurar que los recursos que cuenta la empresa sean utilizados de la forma como se encuentre estipulada en la organización, así como controlar que la modificación solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización. (ISOTOOLS, 2015).

La seguridad de la información se entiende busca preservar las siguientes características:

- Confidencialidad: garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma. (NTC-ISO /IEC 27001, 2013)
- Integridad: salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento. (NTC-ISO /IEC 27001, 2013)

- Disponibilidad: garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran. (NTC-ISO /IEC 27001, 2013)
- Autenticidad: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades. (NTC-ISO /IEC 27001, 2013)
- Auditabilidad: define que todos los eventos de un sistema deben poder ser registrados para su control posterior. (NTC-ISO /IEC 27001, 2013)
- Protección a la duplicación: consiste en asegurar que una transacción sólo se realiza una vez, a menos que se especifique lo contrario. Impedir que se grabe una transacción para luego reproducirla, con el objeto de simular múltiples peticiones del mismo remitente original. (NTC-ISO /IEC 27001, 2013)
- No repudio: se refiere a evitar que una entidad que haya enviado o recibido información alegue ante terceros que no la envió o recibió. (NTC-ISO /IEC 27001, 2013)
- Legalidad: referido al cumplimiento de las leyes, normas, reglamentaciones, disposiciones a las que está sujeto la entidad. (NTC-ISO /IEC 27001, 2013)

La participación en seguridad de la información debe ser constante por todos los funcionarios de una organización con el fin de poder preservar la confidencialidad, la integridad, la disponibilidad, autenticidad y trazabilidad, entre otros principios.

4.2.2 Gestión de Seguridad de la Información

Es un proceso que las organizaciones realizan para descubrir amenazas que pudieran existir y que podrían impactar sus activos de información aprovechándose de vulnerabilidades que posean, colocando en riesgo su disponibilidad, integridad y confidencialidad.

La forma de utilizar las medidas de seguridad es establecer los procesos de seguridad y determinar sus responsables, esto es una orientación basada en procesos dentro de los estándares de gestión según la norma ISO 27001. Para saber que los controles de aseguramientos de la información trabajen para lo que fueron contratados se debe tener un enfoque bien claro sobre quien cae la responsabilidad de sus funcionamientos y que se debe hacer si alguno de ellos pueda fallar en un momento cualquiera. (ISOTOOLS, 2015)

Es de anotar que los controles de seguridad de la información no son sólo técnicas que se instauran, deben estar alineados a la tecnología de la información existente. Es posible fijar varios tipos de controles, como puede ser la documentación de un procedimiento que es un control de la organización y a su vez también se puede implantar una herramienta de software que es un control de tecnología de la información, y de manera complementaría, pero fundamental se requiere la formación de funcionarios que es un control de recursos humanos.

Al erigir un sistema de gestión de seguridad de la información se delinean un conjunto de reglas de seguridad de la información, quienes son los responsables de la seguridad y cuales son controles que se adaptan para proteger la información, por tanto, se puede afirmas que un SGSI es un conjunto reglado de procesos relacionados entre sí, que tienen como objetivo ofrecer seguridad a los activos de información de la entidad.

4.2.3 Sistema de Gestión de Seguridad de la Información

El sistema de gestión de la información, SGSI, es un conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000, 2013).

El modelo de gestión de la seguridad tiene como objeto planificar y crear procedimientos adecuados, para luego implementar controles de seguridad basados en una evaluación de riesgos y consiguiendo mediciones de eficiencia de estos.

Al establecer las políticas de seguridad y los procedimientos en relación con los objetivos del negocio de la empresa, y tener como objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir, se empieza a hablar de un SGSI.

Entre los beneficios que puede otorgar un SGSI se tienen:

- Establece una metodología estructurada para la gestión de seguridad.
- Se puede reducir el riesgo pérdida de la información importante de la organización.
- Hay acceso a la información por parte del cliente con medidas de seguridad.
- Se revisan periódicamente los riesgos y los controles que se apliquen.
- Hay confianza de los clientes y los socios de la empresa.
- Se realizan auditorías externas para ayudar a identificar las debilidades del SGSI encontrando que áreas se deben mejorar.
- Se facilita la integración con otros sistemas de gestión.
- Se garantiza la continuidad de negocio tras incidentes graves.
- Cumplimiento con la legislación vigente sobre información personal, propiedad intelectual y demás.
- Mejora la imagen de la organización a nivel nacional o internacional.
- Se producen reglas claras para los funcionarios de la empresa.
- Reduce los costos y mejoras de los procesos y el servicio.
- Produce motivación y satisfacción del personal de la organización.
- Aumenta la seguridad en base la gestión de procesos en vez de compras sistemáticas de productos y tecnologías. (PMG-SSI, 2017)

4.2.4 Normas Familia ISO/IEC 27000

La norma internacional ISO 27000 se compone de una serie de estándares desarrollados, hay otras que todavía están en desarrollo, por la International Organization for Standardization e International Electrotechnical Commission, todos estos conjuntos de normas proporcionan un marco de gestión de la seguridad de la información y cualquier organización o empresa las pueden utilizar

El organismo encargado de normalizar este tipo de normas en Colombia es el ICONTEC (Instituto Colombiano de Normas Técnicas y Certificaciones).

A continuación, se darán a conocer algunas normas de ISO/IEC 27000.

- ISO/IEC 27000: Es la norma que general que recoge todas las definiciones sobre las normas que la componen, donde indica el alcance y propósito de cada una de ellas, también se encuentran descripciones y conceptos sobre el SGSI. Fue publicada el 01/05/2009 y tiene su última versión el 14/01/2014.
- ISO/IEC 27001: Esta es la norma primordial de todas en la serie y contiene todos los requisitos de SGSI, compuesta por el Anexo A, donde se enumera resumida los objetivos de control y controles a desarrollar en la norma ISO 27002. Se publica el 15 de octubre de 2005, y su última revisión el 25 de septiembre de 2013 y es certificable.
- ISO/IEC 27002: Esta norma es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en la seguridad de la información, Contiene 39 objetivos

de control y 133 controles agrupados en dominios. Nace el primero de julio de 2007 y no es certificable.

- ISO/IEC 27003: Esta norma es la guía que se concentra en los detalles críticos que se necesitan para el diseño e implementación de un SGSI para que sea exitoso. Esta norma se dio a conocer el primero de febrero de 2010 la cual no es certificable.
- ISO/IEC 27004: Esta norma se creó para utilizar procedimientos de medidas que pueden determinar la eficacia del SGSI y de todos los controles implementados. Publicada el 15 de diciembre de 2009.
- ISO/IEC 27005: Esta norma proporciona criterios para la gestión del riesgo en la seguridad de la información de las organizaciones. Publicada el primero de junio de 2011 y no es certificable.
- ISO/IEC 27006: La norma específica los requisitos para la acreditación de entidades de auditorías y certificación de SGSI. Fue dada a conocer el primero de diciembre de 2011 y no es certificable.
- ISO/IEC 27035: La norma proporciona una guía sobre la gestión de incidentes de seguridad de la información. Se dio a conocer el 17 de agosto de 2011. Y otras más que se encuentran en el portal de ISO 2700 en español y su referencia de búsqueda se encuentra en el apartado de la bibliografía. (ISO2700.ES, 2018).

Es de anotar que ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas

del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

4.2.5 Modelo de Seguridad y Privacidad de la Información MSPI

El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL:TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

Según el MINTIC este MSPI se actualiza periódicamente según la normativa 27001, la ley de protección de datos personales, transparencia y acceso a la información pública, con el fin de estar acorde con todas estas legislaciones en gestión de la información.

A nivel metodológico cuenta con varias guías anexas que ayudaran a las entidades seguir detalladamente las fases del modelo, y poder comprender a su vez los resultados obtenidos por cada etapa desarrollada.

El MINTIC desarrolla este modelo para que las entidades del estado tengan una guía, contribuyendo transparencia en gestión pública, y promoviendo el uso de las mejores prácticas de protección de la información.

Las guías que proporcionan el modelo son las siguientes:

- Guía 1 - Metodología de pruebas de efectividad
- Guía 2 - Política General MSPI v1
- Guía 3 - Procedimiento de Seguridad de la Información
- Guía 4 - Roles y responsabilidades
- Guía 5 - Gestión Clasificación de Activos
- Guía 6 - Gestión Documental
- Guía 7 - Gestión de Riesgos
- Guía 8 - Controles de Seguridad de la Información
- Guía 9 - Indicadores Gestión de Seguridad de la Información
- Guía 10 - Continuidad de Negocio
- Guía 11 - Análisis de Impacto de Negocio
- Guía 12 - Seguridad en la Nube
- Guía 13 - Evidencia Digital (En actualización)
- Guía 14 - Plan de comunicación, sensibilización, capacitación
- Guía 15 - Auditoria

- Guía 16 - Evaluación de Desempeño
- Guía 17 - Mejora continua
- Guía 18 - Lineamientos terminales de áreas financieras de entidades públicas
- Guía 19 - Aseguramiento de protocolo IPv4_IPv6
- Guía 20 - Transición IPv4_IPv6
- Guía 21 - Gestión de Incidentes (MINTIC, 2017)

El Modelo de Seguridad y Privacidad de la Información, MSPI del MINTIC, está basado en la norma ISO/IEC 27000 vigentes, y se encuentra en su versión 3.0.2 del 29 de julio de 2016. Su uso está orientado a las entidades públicas de orden nacional y territorial, a proveedores de servicios de Gobierno en Línea, o puede ser adoptado por cualquier empresa que así lo desee, siendo el componente transversal a la estrategia GEL, que sustenta al componente de TIC para la gestión en el uso estratégico de las tecnologías de la información proporcionándole un modelo de seguridad orientado a salvaguardar la confidencialidad, integridad y disponibilidad de la información, y de esta forma permite que la entidad alcance sus objetivos y el cumplimiento de la misión. Asimismo, La Seguridad y Privacidad de la Información está presente en componente de TIC para Servicios soportando el manejo de la información manejada en los diferentes servicios que brinda la Entidad, colocando especial atención en las normas sobre protección de datos personales, con el fin de salvaguardar el derecho a la intimidad. (Ministerio de las Tecnología y las Comunicaciones, 2017).

El modelo busca que la tecnología contribuya al mejoramiento de la gestión apoyando los procesos para alcanzar una mayor eficiencia y transparencia en su ejecución, para que facilite la administración y el control de los recursos y brinde información objetiva y oportuna para la toma de decisiones en todos los niveles. Permite la alineación de la gestión de TI con los objetivos estratégicos de la entidad, el aumento la eficiencia de la organización y la mejora de la forma como se prestan los servicios misionales.

4.2.6 Modelo Bell-LaPadula

Modelo multinivel propuesto para fortalecer el control de acceso en aplicaciones militares y del gobierno. En estas aplicaciones, generalmente los sujetos son divididos en diferentes niveles de seguridad. Un sujeto puede acceder a objetos hasta ciertos niveles, determinado por su nivel de 2 seguridad, por ejemplo: no cualquiera podría tener acceso a información clasificada como top secret.

El modelo Bell-Lapadula es un modelo enfocado en la confidencialidad y define dos reglas de control de acceso mandatorio (MAC) y una regla de control de acceso discrecional (DAC) con tres propiedades de seguridad:

- La propiedad de seguridad simple: un sujeto en un nivel de seguridad dado no puede leer un objeto de un nivel de seguridad mayor.
- La propiedad estrella: un sujeto en un nivel de seguridad dado no puede escribir en algún objeto de un nivel de seguridad menor.
- La propiedad de seguridad discrecional: el uso de una matriz de acceso para especificar el control de acceso discrecional. (CISSP, 2018)

4.2.7 Modelo de BIBA

Modelo que describe un conjunto de reglas de control de acceso diseñadas para asegurar la integridad de los datos, los datos y los sujetos son agrupados en niveles ordenados de integridad. El modelo se diseñó para que los sujetos no puedan acceder a objetos en un rango superior al de ellos o a objetos de menor rango.

El modelo de Biba es similar al de Bell-Lapadula, pero este no puede leer hacia abajo ni escribir hacia arriba y además se diferencian en que este se concentra en la integridad de los datos. El modelo se basa en que la preservación de la integridad de los datos tiene tres objetivos:

- Prevenir la modificación de datos por entes no autorizados
- Prevenir la modificación de datos no autorizados por entes autorizados
- Mantener la consistencia interna y externa. (CISSP, 2018)

Este modelo se basa también en tres conjuntos: los sujetos, que poseen un grado de autorización, los objetos, que tienen una calificación de seguridad, y la matriz de control de acceso, que contiene los derechos discrecionales. Se admite que una información puede fluir entre los sujetos de sus grados de autorización, y hacia los superiores; así, la información que tenga la calificación mínima puede llegar a todos, y la de máximo no puede salir de su nivel.

Igualmente, un sujeto no puede acceder a objetos de grado superior al suyo, y no puede generar información con una calificación menor que la suya para impedir que transfiera secretos a sujetos con menos autorización. Como ejemplo, en algunos ámbitos se establece para los documentos una jerarquía de seguridad con cuatro grados: sin clasificar, confidencial, secreto y máximo secreto. En este entorno se aplica un principio de seguridad en el cual cada sujeto tiene un grado de autorización determinado, y puede leer todos los documentos cuya calificación sea menor o igual que la que corresponda a ese grado.

4.2.8 El Modelo Clark & Wilson

Modelo que se preocupa por la integridad de la información, usando políticas de integridad que definen reglas de aseguramiento y reglas de certificación. El principio básico de este modelo se encuentra bajo la idea de una transacción que es un conjunto de operaciones. Un artículo restringido es considerado una información clave en este modelo, un procedimiento de verificación de integridad asegura que todos los artículos restringidos son válidos. Los procedimientos de transformación son las transacciones que fuerzan la política de integridad.

Está enfocado en tres objetivos de integridad: previene que usuarios no autorizados realicen modificaciones, mantiene la consistencia interna y externa, y previene que usuarios autorizados realicen modificaciones inapropiadas, por tanto, no se puede modificar inapropiadamente mientras se están realizando cambios y todas las modificaciones son registradas, manteniendo la

consistencia de la integridad de los datos. Propende proteger la integridad de los datos. (CISSP, 2018).

Este es un modelo de seguridad que está diseñado para entornos comerciales y se enfoca a la integridad de la información, existen tres características que son de mayor relevancia tanto al sector comercial y al sector militar, estos son: confidencialidad, integridad y disponibilidad. Debido a los modelos formales de seguridad que maneja el sector militar la confidencialidad ha sido de gran impacto ya que la meta primordial es la prevención de revelación de información. Sin embargo, la seguridad del sector comercial está más enfocada a la integridad de la información ya que su impacto está dirigido a la protección de modificaciones inadecuadas de los datos por personas autorizadas o no autorizadas, realizando esta comparación se puede determinar que la integridad juega un rol de mayor relevancia en los sistemas comerciales de computo relacionados con operaciones de negocio y control de los recursos, más que la confidencialidad. Las políticas de integridad se enfocan en dos controles que son primordiales en el mundo comercial; el primero es de “transacciones correctas” y el segundo de “separación de obligaciones.”

En cuanto a las transacciones correctas se pretende garantizar que un usuario no pueda modificar información arbitrariamente, solo permite la modificación de algunos registros de manera determinada, a su vez el control de separación de obligaciones como objetivo primordial es mantener la consistencia de la información al separar las operaciones que deben ser realizadas por diferentes sujetos

5. Diseño Metodológico

El proyecto se basa en las siguientes metodologías para su desarrollo:

5.1 Ciclo PHVA

Es una herramienta de gestión presentada en los años 50 por el estadístico estadounidense Edward Deming, más conocida como el ciclo PHVA (Planificar, Hacer, Verificar y Actuar):

Planificar: En esta etapa se proyectan los objetivos a alcanzar y se verifican los procesos vitales para conseguir los resultados acordes a las políticas de la entidad. Igualmente se determinan también los parámetros de medición a ejecutar para el control y seguimiento de los procesos.

Hacer: Se realiza la implementación de los cambios o acciones con el fin de instaurar las correcciones planificadas. Con el objeto de ser eficaces y poder subsanar ligeramente posibles errores en la ejecución, por lo general se efectúa un plan piloto a modo de prueba o testeo.

Verificar: Con el plan de mejoras en ejecución, se fija un lapso de prueba para conocer la efectividad de los cambios procediendo a su medición, que permite ajustar las correcciones planteadas.

Actuar: Una vez realiza la verificación y de existir ajustes que de no realizarse interferirían con la consecución de los objetivos definidos, se proceden a hacer efectivas dichas correcciones,

tomando las medidas adecuadas para optimiza el desarrollo de los procesos. (ISOTOOLS, 2015). Se observa en la figura 4 una imagen del ciclo PHVA:

Figura 4. Ciclo PHVA

Adaptado de Aulafacil (2017). Tomado de: https://www.aulafacil.com/cursos/administracion/gestion-de-la-calidad/el-ciclo-phva-l35719

5.2 Marco MSPI

Asimismo, este ciclo es adoptado por gobierno colombiano al proponer el marco de implementación donde propone 5 fases: Diagnóstico, Planificación, implementación, Gestión y Mejora Continua, donde el presente proyecto aplicado, abarca la fase de planificación del PHVA, que corresponde a la etapa de Diagnóstico y planificación del modelo MSPI, como se observa en la figura 5:

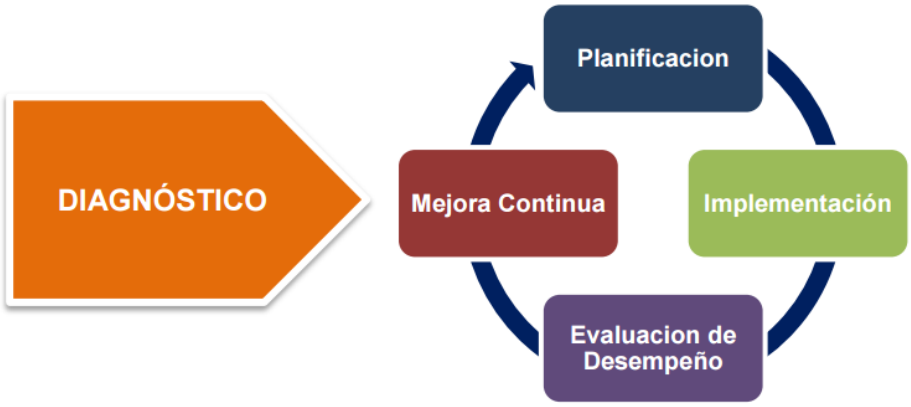


Figura 5. Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información
Adaptado del Modelo de Seguridad y Privacidad de la Información, MINTIC. (2016). Tomado dehttps://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Para la fase de Diagnóstico se toma la siguiente secuencia según la metodología propuesta por el modelo de seguridad y privacidad de la información del MINTIC, la cual se observa en la siguiente figura 6:

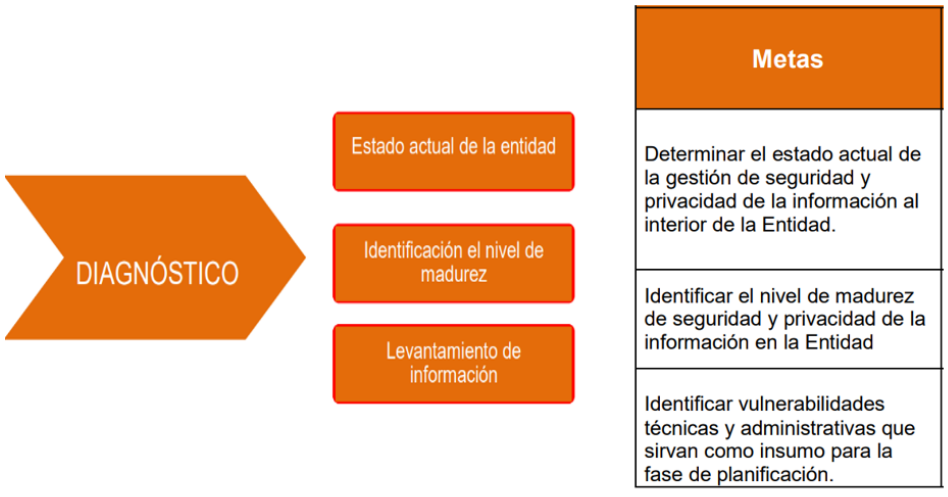


Figura 6. Metas Fase de Diagnóstico
Adaptado del Modelo de Seguridad y Privacidad de la Información, MINTIC. (2016). Tomado dehttps://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Asimismo, para la etapa de planificación se efectúa con base en el modelo mencionado y el cual se refleja en la siguiente imagen:

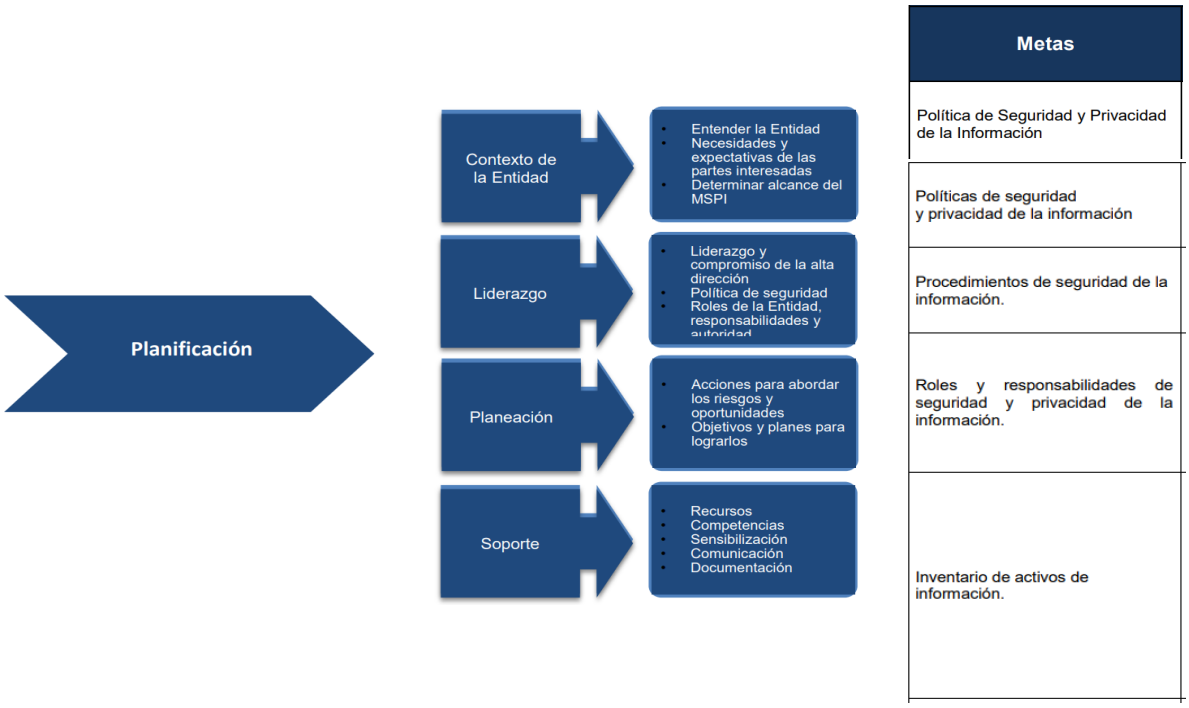


Figura 7. Metas Fase de Planeación
Adaptado del Modelo de Seguridad y Privacidad de la Información, MINTIC. (2016). Tomado dehttps://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Por otra parte, y teniendo en cuenta que el contexto organizacional del MSPI en sí, son las entidades del Estado, la metodología en la cual se basa gestión del riesgo es la guía que propone el Departamento de la Función Pública, DAFP, buscando que haya una integración a lo que se ha desarrollado dentro de la Entidad para otros modelos de Gestión, y de este modo aprovechar el trabajo adelantado en la identificación de Riesgos para ser complementados con los Riesgos de Seguridad.

6. Resultados y Discusión

6.1 Desarrollo Fase De Diagnóstico

En esta fase se pretende identificar el estado actual de la organización con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información, para lo cual se realiza las siguientes actividades:

6.1.1 Métodos de Recolección de Información

6.1.1.1 Observación Directa

Con el fin de conocer personalmente el entorno físico y humano donde se desarrollan las actividades, se procede a realizar visitas a todas las dependencias del Hospital, en compañía de la asesora de calidad de la Institución, durante las cuales también se constata la existencia de los activos de información y las falencias físicas de seguridad que se puedan presentar en los dispositivos, sistemas, red y documentos, y que podrían ser explotadas por una amenaza interna o externa.

6.1.1.2 Entrevistas Informales

Se sostiene diálogos en los cuales se efectúan preguntas abiertas al gerente de la entidad y a los encargados de las oficinas de informática, de control interno y de calidad principalmente, por ser

los funcionarios que recogen información relacionada con el tema de tecnología de la información y conocen de eventos e incidentes de seguridad que se hayan presentado en el Hospital.

También se realiza charlas esporádicas con coordinadores de las áreas misional y de apoyo quienes con su punto de vista pueden coadyuvar a identificar debilidades y amenazas en los activos de información que administran.

6.1.1.3 Encuesta Sobre Seguridad

Con el fin de identificar vulnerabilidades y amenazas que puedan estar presentes en las diferentes dependencias del Hospital, como también tener una visión sobre lo comprendido en seguridad y privacidad de la información por parte de los servidores públicos, se realizan 10 encuestas estructuradas a funcionarios escogidos aleatoriamente en el Hospital de las siguientes áreas: uno (01) de Hospitalización; uno (01) de Jurídica; uno de (01) de Control de Calidad; uno (01) Contabilidad; uno (01) de Contratación; uno (01) de Laboratorio; uno (01) de archivo; uno (01) de Urgencias; uno (01) de Farmacia ; y uno (01) de Facturación.

Siendo esta una manera efectiva que permite identificar el porqué de las implementaciones de seguridad y sus controles en la entidad, si existieren, comprobando además si los encuestados comprenden los procesos de seguridad, si se ha tomado conciencia de las políticas de seguridad y la percepción que poseen sobre algunas amenazas y vulnerabilidades de la Entidad. (Guía para la Gestión y Clasificación de Activos de Información, MINTIC, 2016).

6.1.1.4 Prueba de Penetración

Se realizan pruebas técnicas de intrusión controlada y autorizada por la gerencia del Hospital a los activos de información que permitan conocer si existen vulnerabilidades en el sistema informático y que eventualmente pueda ser aprovechada por una persona externa a la Entidad, sin conocimientos profundos en el tema, usando solamente un computador portátil y un sistema operativo ideado para este fin.

6.1.2 Levantamiento De Información

Durante la ejecución de esta actividad se debe allegarlos datos que permitan identificar los activos más importantes del Hospital, relacionados con los procesos de esta, ya sea misionales o de apoyo. También debe permitir conocer el contexto de la entidad, es decir, el entorno donde se proyectan los objetivos de la entidad.

Las tareas para realizar son reconocer el organigrama de la entidad, mapa de procesos, políticas de seguridad, manual de políticas, metodología de riesgos, identificación de riesgos, planes de gestión de riesgos, entre otros, esta información es la base para la identificación de la brecha de seguridad que tiene la entidad.

En esta fase también se debe identificar los grupos de interés, al interior de la entidad, como lo es control interno, tecnología, recursos humanos, calidad, comunicaciones, GEL, líderes de procesos. (Guía Metodológica de Pruebas de Efectividad, MINTIC, 2016).

6.1.2.1 Organigrama

En la figura 8 se observa el organigrama existente de la institución:

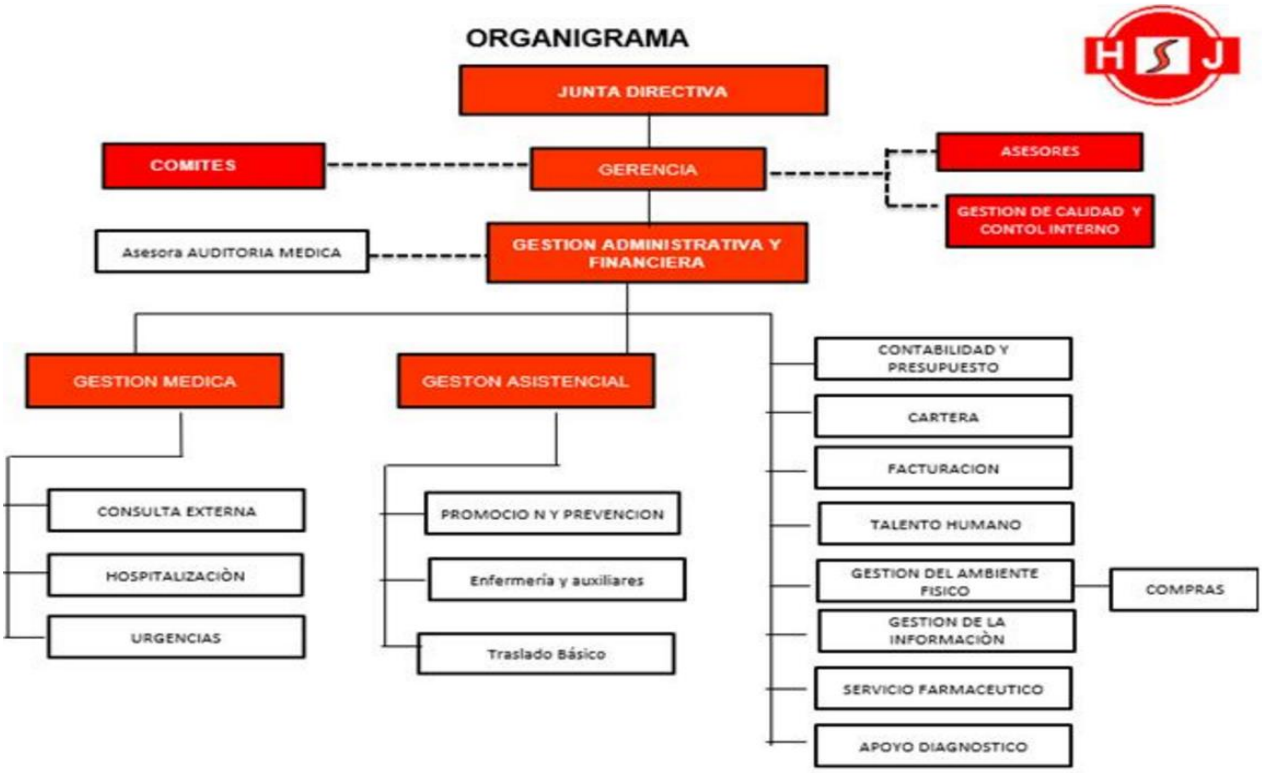


Figura 8. Organigrama del Hospital San José de Ortega.
Adaptado de Pagina Web Hospital San José de Ortega (2017). Tomado dehttp://hospitalsanjoseortega.gov.co/es/acerca-de-la-entidad/estructura-organizacional

La estructura organizacional del Hospital San José de Ortega está compuesta por un órgano superior denominado junta directiva, conformada por cinco miembros: el alcalde del municipio, el gerente del hospital, un representante de los usuarios y dos representantes de los empleados, el cual solo ejerce sus funciones mediante sesiones esporádicas programadas; descendentemente está ubicado el gerente, quien se apoya en los comités creados con tareas específicas y los asesores de jurídica, gestión de calidad y control interno. El subalterno jerárquico del gerente es el gestor

administrativo y financiero, conocido como el "administrador del hospital", quien es asesorado por el auditor médico y tiene a cargo ocho oficinas para el cumplimiento de su labor, siendo estas: contabilidad y presupuesto, cartera, facturación, talento humano, gestión del ambiente físico, gestión de la información, servicio farmacéutico, apoyo diagnóstico. Asimismo, el administrador del hospital tiene a cargo las dos dependencias siendo la primera la de gestión medica con sus áreas de consulta externa, hospitalización y urgencias, y la segunda gestión asistencial con sus áreas de promoción y prevención, enfermería y auxiliares, y traslado básico.

6.1.2.2 Mapa de proceso

En la figura 9 se observa el mapa de procesos del hospital San José de Ortega:

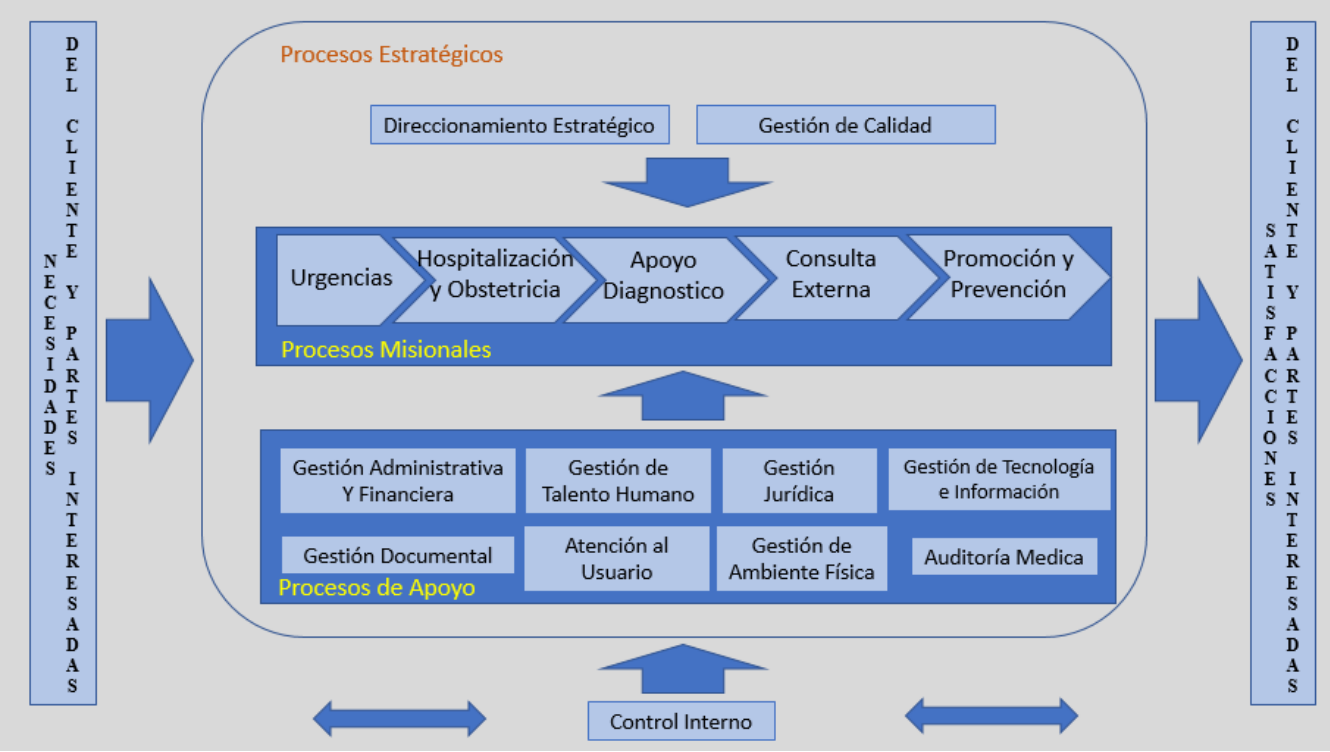


Figura 9. Mapa de Procesos Hospital San José de Ortega
Adaptado del Manual de Gestión de Calidad Hospital San José de Ortega (2017)

El Hospital San de Ortega con el fin de satisfacer las necesidades de sus clientes realiza un macroproceso estratégico dirigido por el gerente de la institución, asistido por sus asesores para lograr los objetivos misionales que se ejecutan en los subprocesos de urgencias, hospitalización y obstetricia, apoyo diagnóstico, consulta externa, y promoción y prevención, los cuales son apoyados por los subprocesos de gestión administrativa y financiera, gestión del talento humano, gestión jurídica, gestión de tecnología e información, gestión documental, atención al usuario, gestión de ambiente físico y auditoría médica. Todos los procesos son supervisados por la oficina de control interno para el mejoramiento del sistema.

6.1.2.3 Políticas de seguridad de la información

Durante esta fase de recolección de datos se conoce que el Hospital San José de Ortega no posee Políticas, como tampoco, procedimientos de Seguridad de la Información, por cuanto verificado los archivos que se encuentran en las oficinas de gestión de la información, secretaria de gerencia, control interno, no se evidencia la existencia de proyectos, actas u otro documento que se refiera al tema de la seguridad de la información.

6.1.2.4 Planes de gestión de riesgos

Respecto a temas de riesgos en la Institución se conoce a través de conversación con diferentes líderes de proceso que no poseen un sistema de Gestión del Riesgo para la Información, existen documentos relacionados con el mapa de riesgos de anticorrupción, únicamente.

Realizando verificación a los datos abiertos contenidos en el Sitio Web Oficial del Hospital, se encuentra un documento, procedente de la oficina de Control Interno, con el título "SEGUIMIENTO A LAS ESTRATEGIAS DEL PLAN ANTICORRUPCION Y ATENCION AL CIUDADANO AÑO 2015" donde de menciona el mapa de riesgos de Anticorrupción.

Asimismo, se halla un archivo, procedente de esta misma Oficina, titulado "SEGUIMIENTO A LAS ESTRATEGIAS DEL PLAN ANTICORRUPCION YATENCION AL CIUDADANO AÑO 2015" donde se menciona que para el año 2015 se publicó un Mapa de Riesgos y el cual sería implementado con los funcionarios que designación como líderes de los procesos.

Siguiendo con la búsqueda en la página Web de la E.S.E., se encuentra un archivo excel, nombrado "programa-y-plan-de-accion-2016-control-interno", donde en una de sus hojas marcada como "riesgos evalúa" se encuentra un mapa de riesgos, el cual en su encabezado dice Gobernación del Tolima, con fecha de actualización octubre de 2008 y corte de fecha de evaluación 31 de octubre de 2010.

6.1.2.5 Infraestructura física y de servicios

El Hospital cuenta con un área total de 3.763 m2, con la distribución reseñada en la **Tabla 01,** donde ofrece los servicios de Nivel I de atención.

Tabla 1. Distribución Consultorios y Servicios

SERVICIO	**CAPACIDAD INSTALADA**
Numero De Consultorios Para Consulta Externa	**6**
Numero De Consultorios Para P Y P (Promoción y Prevención)	**2**
Numero De Consultorios Odontológicos	**1**
Numero De Consultorios Para Vacunación	**1**
Numero De Consultorios Urgencias	**2**
Numero De Consultorios De Consulta Prioritaria	**1**
Numero De Camillas Adulto Urgencias	**3**
Numero De Salas De Procedimientos	**1**
Numero De Salas De Partos	**1**
Numero De Camas De Hospitalización Adulto	**12**
Numero De Camas De Hospitalización Pediátrica	**4**
Numero De Camas De Hospitalización Obstetricia	**2**
Numero De Ambulancias Básicas	**2**

Nota: Adaptado de Folleto de Portafolio de Servicios del Hospital San José de Ortega (2017)

- Consulta externa: 6 consultorios habilitados para medicina general
- Dos consultorios para programas especiales de enfermería
- Un consultorio de odontología con 2 unidades odontológicas fijas
- Un laboratorio clínico totalmente dotado
- Urgencias: 2 consultorios dotados, 1 sala de procedimientos, 1 sala de observación.

- Hospitalización: 18 camas distribuidas en habitaciones uní y bipersonales.
- Sala de partos: 1 sala de partos
- Transporte Básico Asistencial: 2 Ambulancias Básicas
- Servicio farmacéutico: 24 HORAS
- Programas de promoción y prevención:

  Planificación Familiar

  Citologías

  Vacunación

  Control gestante, del niño, del joven y el adulto.

6.1.2.6 Talento humano áreas de servicios

Para prestar los servicios ofertados el hospital San José de Ortega cuenta con el personal descrito en la **Tabla 02:**

Tabla 2. Personal Área de Servicios del Hospital

TALENTO HUMANO	***CANTIDAD***
Número De Médicos Generales	9
Número De Médicos Rurales	3
Numero De Odontólogos	2
Numero De Bacteriólogos	2
Numero De Enfermeros	3
Numero De Auxiliares De Enfermería	22

Numero De Auxiliares De Odontología	1
Numero De Auxiliares De Laboratorio	1
Numero De Higienista Orales	1
Número De Conductores De Ambulancia	4

Nota: Adaptado de Portafolio de Servicios del Hospital (2017)

6.1.3 Activos De Información

La identificación del inventario de activos de información permite clasificar los activos a los que se les debe brindar mayor protección, pues identifica claramente sus características y rol al interior de un proceso.

Las actividades por realizar para obtener un inventario de activos son definición, revisión, actualización y publicación, las cuales se reflejan documentalmente en la Matriz de Inventario y Clasificación de Activos de Información. Es de anotar que el Hospital aún no ha definido los activos de información que posee la Entidad, si bien en la oficina de gestión de información existe un archivo en excel con dispositivos conectados a la red, éste solamente se limita a los activos electrónicos sin su debida clasificación y tampoco se refiere a los documentos físicos y digitales institucionales, o sea no cuenta con un inventario riguroso de activos de información, por tanto, las actividades de revisión y actualización no se pueden realizar durante la ejecución dentro del presente proyecto. (Guía para la Gestión y Clasificación de Activos de Información, MINTIC, 2016).

6.1.3.1 Formato de recolección.

Con base en los lineamientos propuestos en la Guía para la Gestión y Clasificación de Activos de Información del MINTIC se diseña el formato excel, como se observa en la figura 8, para la recolección de Información con los siguientes campos:

- Identificador: Número consecutivo único que identifica al activo en el inventario.
- Proceso: Nombre del proceso al que pertenece el activo.
- Nombre Activo: Nombre de identificación del activo dentro del proceso al que pertenece.
- Descripción/Observaciones: Es un espacio para describir el activo de manera que sea claramente identificable por todos los miembros del proceso.
- Tipo: Define el tipo al cual pertenece el activo. Para este campo se utilizan los siguientes valores:
  - ✓ Información: Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
  - ✓ Software: Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.

- ✓ Recurso humano: Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
- ✓ Servicio: Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- ✓ Hardware: Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
- ✓ Otros: activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso.

❖ Ubicación: Describe la ubicación tanto física como electrónica del activo de información.

❖ Clasificación: Hace referencia a la protección de información de acuerdo con Confidencialidad, Integridad y Disponibilidad.

❖ Justificación: Para cada valoración, describe el impacto que causaría la pérdida de la propiedad (Confidencialidad, Integridad y Disponibilidad), o el argumento del porque se asignó dicha valoración.

❖ Criticidad: Es un cálculo automático que determina el valor general del activo, de acuerdo con la clasificación de la Información:

- ✓ Alta. Activos de información en los cuales la clasificación de la información en dos o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.

- ✓ Media. Activos de información en los cuales la clasificación de la información es alta en una de sus propiedades (confidencialidad, integridad, y disponibilidad) o al menos una de ellas es de nivel medio.
- ✓ Baja. Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

- ❖ Propiedad
  - ✓ Propietario: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con el proceso se clasifican adecuadamente. Deben definir y revisar periódicamente las restricciones y clasificaciones del acceso.
  - ✓ Custodio: Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de hacer efectivos las restricciones y clasificaciones de acceso definidos por el propietario. (Para sistemas de información o información consignada o respaldada, generalmente es TI o para información física, los custodios pueden ser los funcionarios o el proceso de archivo o correspondencia, el custodio generalmente se define donde reposa el activo original).

- ❖ Acceso

- ✓ Usuarios: Son quienes generan, obtienen, transforman, conservan, eliminan o utilizan la información, en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información.

Para la recolección de la información acorde con los puntos anteriores se utiliza el formato que se observa en la figura 10:

Hospital San Jose de Ortega, E.S.E.

Definición de Activos de Información

Fecha:

Elaboró:

Identificador	Proceso	Nombre Activo	Descripción	Tipo						Ubicación	Clasificación	Justificación	Propiedad		Acceso	Criticidad		
				Información	Software	Recurso humano	Servicio	Hardware	Otro				Propietario	Custodio		Alta	Media	Baja

Figura 10. Formato Definición de Activos de Información

6.1.3.2 Definición.

La definición consiste en determinar qué activos de información van a hacer parte del inventario, con este fin se realiza una visita por cada una de las dependencias del Hospital donde se dialoga con los líderes de cada proceso para conocer que activo (Información, Software, Recurso Humano, Servicio, Hardware u otro) podría hacer parte del inventario, además se realiza una inspección visual para constatar de que algún otro activo importante quede excluido del inventario. En la siguiente figura se observa una impresión diligenciada del formato usado:

Hospital San Jose de Ortega, E.S.E.

Definición de Activos de Información

Fecha: 17 DE ABRIL DE 2017

Elaboró:

Identificador	*Proceso*	*Nombre Activo*	*Descripción*	*Tipo*						*Ubicación*
				Información	*Software*	*Recurso humano*	*Servicio*	*Hardware*	*Otro*	
SIN	HOSPITALIZACION	Consentimiento Informado de Retiro Voluntario		X						HOSPITALIZACION
HSJ-PA-AU-FO-06	HOSPITALIZACION	Consentimiento Informado de Cateterismo Vesical		X						HOSPITALIZACION
SIN	HOSPITALIZACION	Hoja de Liquidación por Paciente y por Dia		X						HOSPITALIZACION
SIN	HOSPITALIZACION	Comprobante de Recibo del Usuario		X						HOSPITALIZACION
SIN	HOSPITALIZACION	Historia Clinica Traslado Asistencial		X						HOSPITALIZACION
SIN	HOSPITALIZACION	Consentimiento Informado Traslado Asistencial		X						HOSPITALIZACION
SIN	HOSPITALIZACION	Tratamientos		X						HOSPITALIZACION
SIN	HOSPITALIZACION	Puerperio Inmediato (2 Primeras Horas)		X						HOSPITALIZACION
SIN	HOSPITALIZACION	Control de Liquidos		X						HOSPITALIZACION
HSJ-PA-AU-FO-07	HOSPITALIZACION	Consentimiento Informado Sonda Nasogastrica		X						HOSPITALIZACION
HSJ-PM-UR-FO-02	HOSPITALIZACION	Formato de Entrega de Turno		X						HOSPITALIZACION
PM-UR-01	HOSPITALIZACION	PROCEDIMIENTO TRIAGE		X						HOSPITALIZACION
PM-TB-FO-03	HOSPITALIZACION	FORMATO DE MANTENIMIENTO AMBULANCIA		X						HOSPITALIZACION
PM-TB-FO-02	HOSPITALIZACION	FORMATO DE CONTROL DE LIMPIEZA Y ASEO AMBULANCIA		X						HOSPITALIZACION
PM-TB-FO-01	HOSPITALIZACION	LISTA DE CHEQUEO AMBULANCIA BÁSICA		X						HOSPITALIZACION
CA-MAN-01	ESTRATEGICO	MANUAL DE PGIRHS		X						DIRECCIÓN
PE-CA-MAN-02	ESTRATEGICO	MANUAL DE BIOSEGURIDAD		X						DIRECCIÓN
PE-CA-MAN-03	ESTRATEGICO	MANUAL DE GESTIÓN DE HISTORIAS CLÍNICAS		X						DIRECCIÓN
PE-CA-MAN-04	ESTRATEGICO	PROGRAMA INSTITUCIONAL DE TECNOVIGILANCIA		X						DIRECCIÓN
PE-CA-MAN-05	ESTRATEGICO	PROGRAMA INSTITUCIONAL DE FARMACOVIGILANCIA		X						DIRECCIÓN
PE-GC-01	ESTRATEGICO	DE LA ATENCIÓN EN LA SALUD (PAMEC)		X						DIRECCIÓN
PA-GD-FO-01	ESTRATEGICO	CONTROL DE DOCUMENTOS		X						DIRECCIÓN
PA-TH-FO-01	TALENTO HUMANO	FORMATO DE ACTA DE CAPACITACION		X						TALENTO HUMANO
PA-SGSST-FO-01	TALENTO HUMANO	FORMATO DE INSCRIPCION COMITÉ COPASST		X						TALENTO HUMANO
PA-SGSST-FO-02	TALENTO HUMANO	SOLICITUD INGRESO A BRIGADA DE EMERGENCIA		X						TALENTO HUMANO
PA-GT-FO-01	SISTEMAS	HOJA DE VIDA EQUIPO DE TECNOLOGIA		X						SISTEMAS
N/A	URGENCIAS	BASE DE DATOS USUARIOS	ALMACENA LOS DATOS BASICOS DE LOS USUARIOS DEL SERVICIOS DE URGENCIAS		X					URGENCIAS
N/A	ESTRATEGICO	BASE DE DATOS RADICACIÓN	CONSERVA LA INFORMACIÓN DE LOS DOCUMENTOS EMITIDOS Y QUE LLEGAN A LA ENTIDAD		X					ESTRATEGICO
N/A	URGENCIAS	COMPUTADOR GENERICO AMD Athlom II X2 270 3.40GHz	ALMACENA LOS DATOS BASICOS DE LOS USUARIOS DEL SERVICIOS DE URGENCIAS					X		URGENCIAS

Figura 11. Screen Formato de Activos Diligenciado

Como se observa en la anterior figura existe documentación que no se encuentra codificada bajo ninguna Norma Técnica, o bien, cuenta con diferentes métodos de codificación. Otro aspecto para resaltar es que el hospital San José de Ortega tiene contratado el servicio que ofrece la Empresa Tecnologías Sinergia S.A.S , por lo cual poseen el Sistema de Información Hospitalario SIHOS WEB, que emite reportes dentro los procesos descritos en la figura 10, ampliando en la figura 11, entre ellos la historia clínica, caja, tesorería, facturación, consulta médica, entre otros, que se deben

considerar dentro de los activos de información de contenido electrónico y como en el caso de la historia clínica no se encuentran de forma física en ninguna de las dependencias, desde que se cuenta con este servicio.

Por otra parte, la Entidad cuenta con cuarenta y seis (46) equipos de cómputo funcionando en sus diferentes áreas operativas y administrativas, los cuales poseen diferentes sistemas operativos de Microsoft desde Windows XP, al actual, Windows 10. En cuanto a equipos que cumplen funciones de servidor, en la sala de sistemas se encuentran un equipo DELL POWEREDGE R420 donde se hospeda el Sistema Hospitalario, también se encuentra un equipo genérico, marca Nation 3000, donde se aloja la base de datos del Sistema de Información Hospitalaria, y otro equipo genérico donde se alojan las copias de seguridad de la base de datos de SIHOS. Es de anotar que algunos equipos no cuentan con licenciamiento y otros equipos portátiles son propiedad del usuario de la red.

Otros inconvenientes percibidos relacionados con la seguridad, es que la Empresa Objeto no cuenta con ningún controlador de dominio en su red, hardware de seguridad (UTM, o firewall perimetral y Sistema de Detección de Intrusos), antivirus corporativo, como tampoco un sistema de cableado estructurado adecuadamente estandarizado, lo que ha obligado a que se instalen dispositivos WIFI y conmutadores en lugares de difícil control, como se observa en las siguientes figuras:

Figura 12. Dispositivo Wifi en uso

Figura 13. Conmutador en Uso Fuera de Área de Control

El hospital posee cuatro (04) cámaras de seguridad distribuidas en los dos pisos y el cuarto de sistemas posee aire acondicionado.

Asimismo, en el sitio web de esta Empresa hacen relación a la seguridad de la Información, en la cual mencionan:

- Datos: El bien intangible más importante de una empresa es la información, por tal motivo, aseguramos la encriptación de las contraseñas del sistema para así evitar la vulneración a la información almacenada. Además, contamos con mecanismos para salvaguardar la integridad de estos con lo cual aseguramos que ninguna persona ajena acceda a los datos del sistema.
- Almacenamiento: Usamos uno de los mejores motores de bases de datos para almacenar la información, con esto aseguramos a nuestros clientes la seguridad, integridad y el rendimiento en la gestión de información de la organización.
- Usuarios: SIHOS WEB permite configurar perfiles para cada usuario de acuerdo con su cargo. Con esta herramienta, se limita la accesibilidad y se brinda la seguridad de que no todos los usuarios manipulan datos sensibles.
- Política de Privacidad: Empleamos cláusulas de privacidad tanto para los clientes como para los empleados de nuestra empresa con lo cual se asegura la absoluta confidencialidad de los datos tanto en su recolección, procesamiento y tratamiento.
- Testing: Antes de lanzar nuestros productos al mercado, estos son sometidos a una serie de pruebas en las cuales nos aseguramos de entregar productos de calidad. Con esto aseguramos un producto íntegro y robusto para el manejo de la información importante de cada organización.

La empresa SIHOS presta servicios administrativos y asistenciales para esta clase de instituciones como se observa en la figura 14:

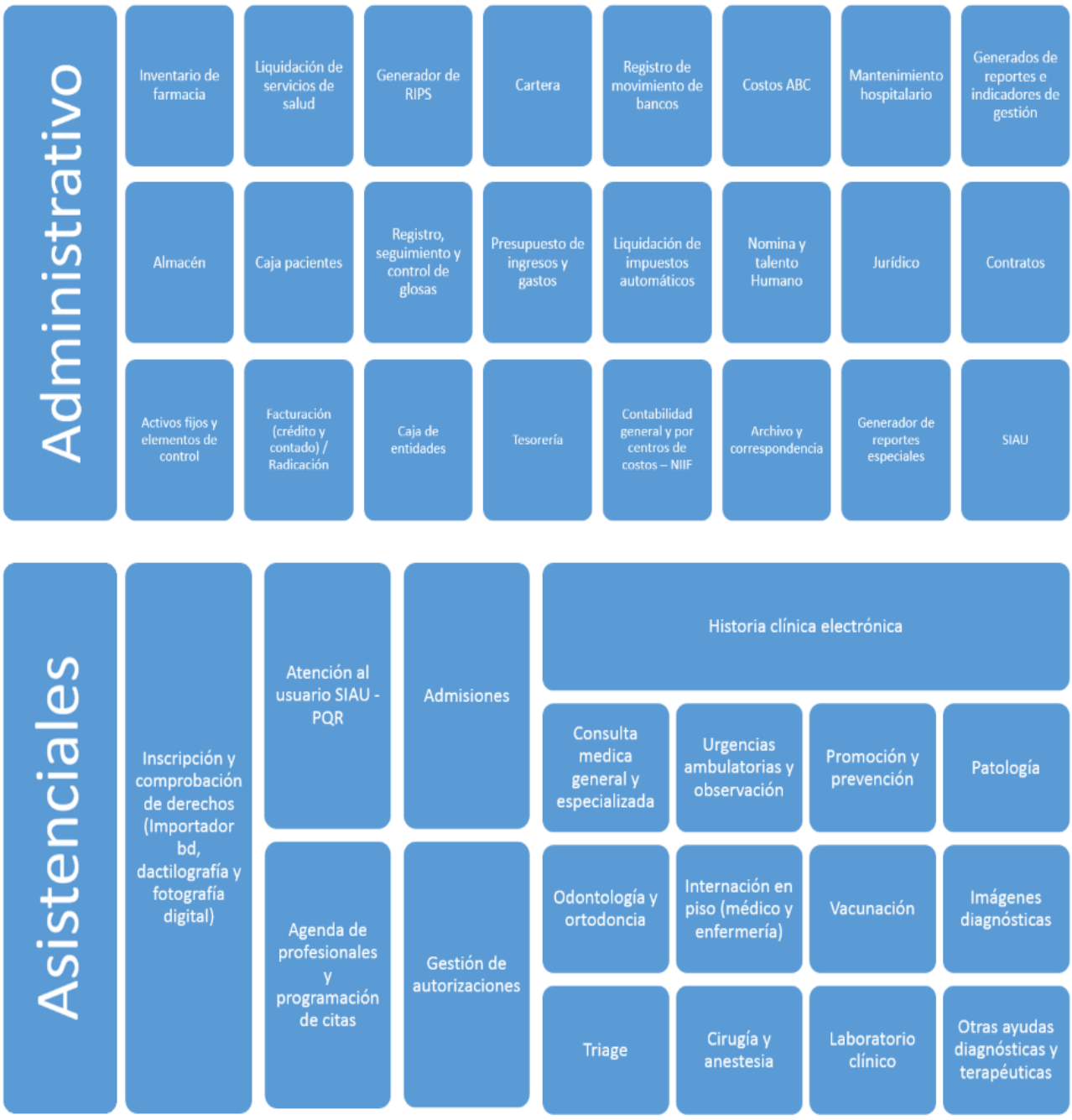


Figura 14. Módulos SIHOS Web
Adapta del Sitio Web Empresa Tecnologías Sinergia S.A.S (2017). Tomado de http://www.sinergia.in/

En la figura 15 se observa un pantallazo del sistema de información SIHOS utilizado en el Hospital:

Figura 15. Screen Ventana SIHOS Reportes

6.1.4 Formato Encuesta de Seguridad.

Teniendo en cuenta que se abordan dos temáticas diferentes, vulnerabilidades y amenazas, y la comprensión que puedan tener los funcionarios sobre seguridad de la información, se procede a

redactar 8 preguntas por cada tema que permitirán comprobar el conocimiento que tienen los empleados del Hospital San José de Ortega con relación al tratamiento de la Seguridad de la Información y una vez obtenido los resultados sirven como insumo para identificar las amenazas y vulnerabilidades que ciernen sobre los activos de información de la entidad.

Los interrogantes se formulan con opciones de respuesta cerrada, con dos o tres opciones para una fácil tabulación de los datos obtener, solamente la segunda pregunta del primer tema y por necesidad de profundización, presenta un punto adicional con ocho opciones de respuesta (Ver Anexo 01). La figura 16 muestra una previsualización de estos formatos:

ENCUESTA DE SEGURIDAD DE LA INFORMACIÓN EN EL HOSPITAL SAN JOSE DE ORTEGA TOLIMA

Fecha: _____

Área: _____

1. ¿Ha recibido en los años 2016 y/o 2017, alguna clase de sensibilización, charla, taller o sensibilización relacionada con temas de Seguridad de la Información, dirigida por el Hospital?

a) Si ☐
b) No ☐

2. Ha tenido algún inconveniente, en los años 2016 y/o 2017, relacionada con perdida de información de propiedad del Hospital?

a) Si ☐
b) No ☐

Si contestó "Si" por favor marque la causa que origina la perdida

a) Virus ☐
b) Hurto ☐
c) Sabotaje ☐
d) Incendio ☐
e) Inundación ☐
f) Olvido Contraseña ☐
g) Falla del Sistema ☐
h) Otro* ☐

*Cual? _____

3. ¿Se realiza periódicamente respaldo de la información importante del Hospital que no está contenida en el SIHOS?

a) Si ☐
b) No ☐

4. ¿En qué medio almacena la información laboral importante de su Área?

a) Dispositivo USB ☐
b) Disco Duro ☐
c) Ambos ☐

5. ¿Utiliza equipos personales (portátil) para realizar su labor del Hospital?

a) Si ☐
b) No ☐

6. ¿Conoce el nombre y contraseña de otros usuarios del SIHOS o computadores de otras áreas?

a) Si ☐
b) No ☐
c) No utiliza ☐

7. ¿Tiene acceso a internet, sin restricciones, en el computador donde guarda la información hospitalaria?

a) Si ☐
b) No ☐

8. ¿Se ha presentado algún inconveniente, este año, que no le haya permitido ingresar a su computador laboral, por más de cuatro horas?

a) Si ☐
b) No ☐
c) No utiliza ☐

II. Tema: Conocimiento de Seguridad y Privacidad de la Información

1. ¿Sabe que son las políticas de seguridad de la información de una entidad?

a) Si ☐
b) No ☐

2. ¿Sabe cuáles son los principales procedimientos de seguridad de la información de una entidad?

c) Si ☐
d) No ☐

3. ¿Conoce cuál es rol que debe desempeñar respecto a la información que administra o usa?

a) Si ☐
b) No ☐

4. ¿Sabe la diferencia entre datos personales públicos, datos personales privados y datos personales sensibles?

a) Si ☐
b) No ☐

5. ¿Conoce quién es el responsable de realizar el respaldo de la información que usted administra?

a) Si ☐
b) No ☐

6. ¿Sabe cómo se construye una contraseña segura para el acceso a sus dispositivos informáticos?

a) Si ☐
b) No ☐

7. ¿Conoce las implicaciones de carácter penal que le acarrearían un uso inadecuado de los datos y los equipos informáticos que usted utiliza con ocasión de su labor en el Hospital?

a) Si ☐
b) No ☐

8. ¿Sabe a qué se refiere el término "Ransomware"?

a) Si ☐
b) No ☐

Figura 16. Formato Encuesta Seguridad.

Después de haber obtenido los datos a través de las preguntas realizadas directamente y consignadas en el formato de encuesta antes descrito se procedió a su tabulación con los resultados que se observan en la siguientes figuras 17,18 y 19, y tablas 3 y 4:

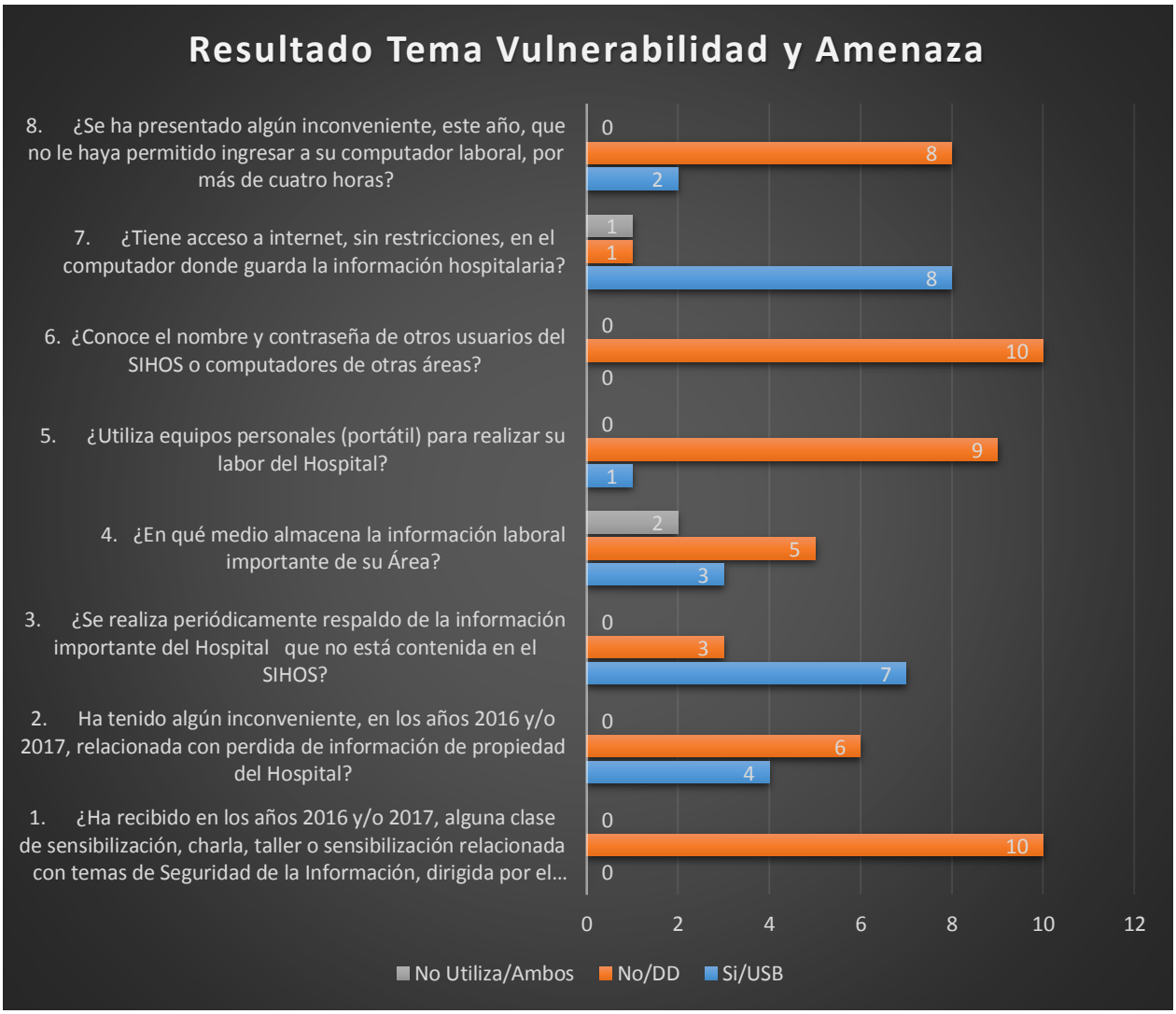


Figura 17. Resultado Tema Vulnerabilidad y Amenaza

Tabla 3. Resultado Tema Vulnerabilidad y Amenaza

Pregunta	***Respuesta***		
	Si/USB	***No/DD***	**No Utiliza/Ambos**

1. ¿Ha recibido en los años 2016 y/o 2017, alguna clase de sensibilización, charla, taller o sensibilización relacionada con temas de Seguridad de la Información, dirigida por el Hospital?	0	10	0
2. ¿Ha tenido algún inconveniente, en los años 2016 y/o 2017, relacionada con pérdida de información de propiedad del Hospital?	4	6	0
3. ¿Se realiza periódicamente respaldo de la información importante del Hospital que no está contenida en el SIHOS?	7	3	0
4. ¿En qué medio almacena la información laboral importante de su Área?	3	5	2
5. ¿Utiliza equipos personales (portátil) para realizar su labor del Hospital?	1	9	0
6. ¿Conoce el nombre y contraseña de otros usuarios del SIHOS o computadores de otras áreas?	0	10	0
7. ¿Tiene acceso a internet, sin restricciones, en el computador donde guarda la información hospitalaria?	8	1	1
8. ¿Se ha presentado algún inconveniente, este año, que no le haya permitido ingresar a su computador laboral, por más de cuatro horas?	2	8	0

Asimismo, se obtiene un resultado independiente de la pregunta de profundización del segundo ítem, el cual se puede observar en la siguiente figura y tabla:

Figura 18. Resultado Pregunta Profundización Encuesta Seguridad Tema 1

Tabla 4. Resultado Pregunta Profundización Encuesta Seguridad Tema 1

Pregunta	***Respuesta***

	Virus	*Hurto*	*Sabotaje*	*Incendio*	*Inundación*	*Olvido Contraseña*	*Falla del Sistema*	*Otro*
Ha tenido algún inconveniente, en los años 2016 y/o 2017, relacionada con pérdida de información de propiedad del Hospital? Si contestó "Si" por favor marque la causa que origina la perdida	3						1	

Se concluye según el resultado del primer tema de la encuesta que el hospital actualmente no ha tomado las medidas necesarias para minimizar los riesgos existentes por la exposición de los activos de información siendo primordial la capacitación del personal sobre temas de seguridad de la información que deriva en el uso de dispositivos personales sin control en las instalaciones de la entidad y al ingreso a sitios web sin restricciones, lo cual puede permitir la propagación del malware que pueden llegar a impactar negativamente la integridad, confidencialidad o disponibilidad de los activos de información de la Entidad.

En cuanto al segundo tema sobre el conocimiento que puedan tener los funcionarios del Hospital San José de Ortega se obtuvo lo siguiente:

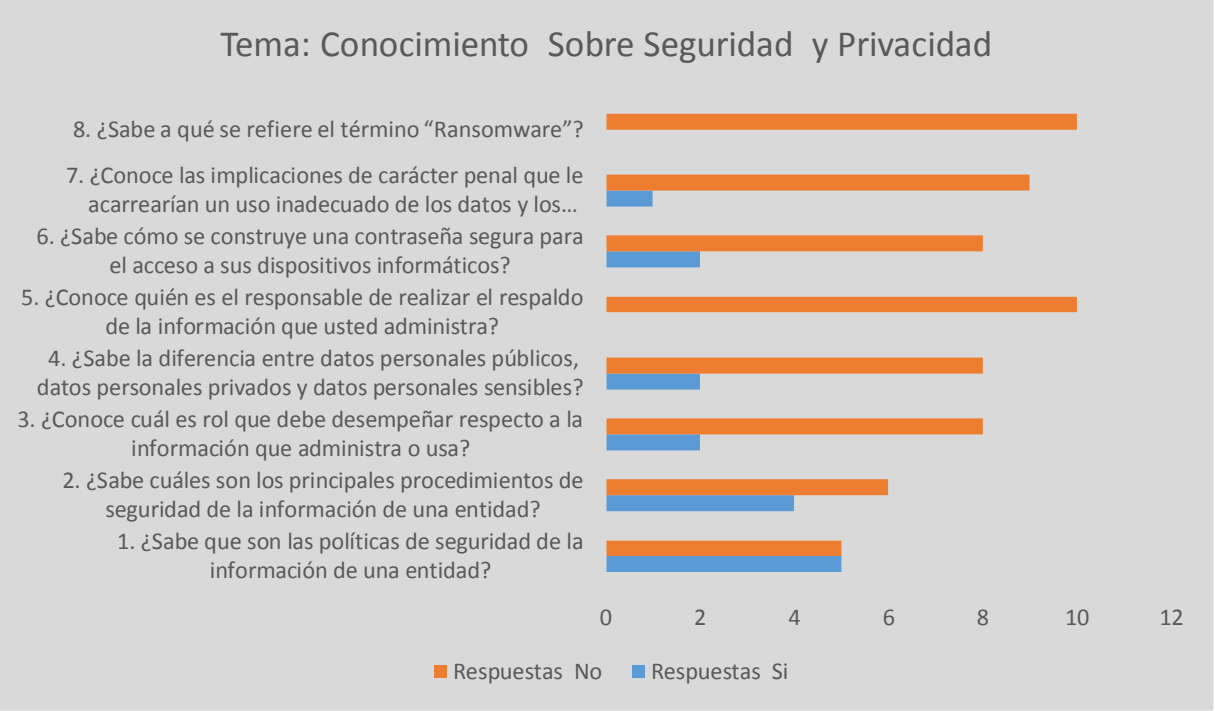


Figura 19. Resultado Tema Conocimiento Seguridad y Privacidad

En la tabla número 5 se refleja el resultado de la encuesta:

Tabla 5. Resultado Tema Conocimiento Seguridad y Privacidad

Pregunta	***Respuestas***	
	Si	***No***
1. ¿Sabe que son las políticas de seguridad de la información de una entidad?	5	5
2. ¿Sabe cuáles son los principales procedimientos de seguridad de la información de una entidad?	4	6
3. ¿Conoce cuál es rol que debe desempeñar respecto a la información que administra o usa?	2	8
4. ¿Sabe la diferencia entre datos personales públicos, datos personales privados y datos personales sensibles?	2	8
5. ¿Conoce quién es el responsable de realizar el respaldo de la información que usted administra?	0	10
6. ¿Sabe cómo se construye una contraseña segura para el acceso a sus dispositivos informáticos?	2	8
7. ¿Conoce las implicaciones de carácter penal que le acarrearían un uso inadecuado de los datos y los equipos informáticos que usted utiliza con ocasión de su labor en el Hospital?	1	9
8. ¿Sabe a qué se refiere el término "Ransomware"?	0	10

Una vez abordado el segundo tema de la encuesta con su respectiva tabulación se obtiene como resultado que es bajo el conocimiento que tienen los trabajadores del Hospital San José de Ortega sobre la temática planteada, derivado esto de su principal vulnerabilidad que es la ausencia de capacitación del personal sobre temas de seguridad de la información y como consecuencia directa de no poseer políticas de seguridad, si bien la mitad de los encuestados manifiesta saber sobre políticas y procedimientos de seguridad de la información es porque han recibido alguna clase de formación en empresas anteriores donde laboraban como lo indicaron al culminar su encuesta, pero la mayoría de los consultados tienen una comprensión muy limitada sobre asuntos relacionados con la seguridad de la información.

6.1.5 Identificación de las Partes Interesadas

Con el fin de determinar cuáles son las personas naturales o jurídicas que se pueden ver afectadas por la implementación del modelo de seguridad de la información en el hospital San José de Ortega se hace un análisis de las necesidades y expectativas que presenta cada una de ellas, para lo cual se dialoga con el gerente, el administrador del hospital, el asesor médico, con un médico rural en turno, con la persona encargada contabilidad y presupuesto, por cuanto hacen parte representativa de los grupos de interés de tipo interno, además conocen las necesidades y expectativas de los grupos de interés externo porque interactúan con ellos, o bien porque reciben sus peticiones, quejas o reclamos. Se presenta en la siguiente matriz el resultado obtenido:

Tabla 6. Partes Interesadas en el MSPI

Tipo	Parte interesada	Necesidades	Expectativas
Interna	Gerente	✓ Cumplir con la normatividad vigente respecto a la seguridad de la información.	✓ lograr un mejor funcionamiento entre los procesos (ahorro gastos), aumento de prestigio por tener implementado un MSPI
Interna	Funcionarios (Procesos Misional y Apoyo)	✓ Obtener capacitaciones sobre el resguardo óptimo de la información. ✓ Disminuir la perdida de información por malware o hurtos. ✓ Fortalecer el manejo de los aplicativos usados en el Hospital. ✓ Evitar la pérdida o fuga de información. ✓ Saber que procedimiento seguir en casos de incidentes de seguridad que se presenten y a quien acudir.	✓ Que el MSPI implantado no obstaculice el normal desarrollo de sus funciones. ✓ Enriquecimiento cognitivo a nivel profesional y personal. ✓ Conseguir respuestas precisas y entendibles relacionadas con las TIC. ✓ Oportunidades de cualificación profesional. ✓ Coordinación entre los servicios ofrecidos a nivel interno y externo.
Externa	Usuario del Proceso Misional	✓ información personal esté protegida según normas.	✓ No presentación de retrasos en la prestación del servicio.
Externa	Hospitales de la Región	✓ Compartir información siguiendo un procedimiento unificado.	✓ Competir bajo condiciones de igualdad.
Externa	Entidades gubernamentales	✓ Prestar apoyo en procesos de formación en TIC ✓ Crear mecanismos para denunciar de delitos cibernéticos.	✓ Cumplimiento de la normatividad. ✓ Entregar periódicamente información acerca de la ejecución del MSPI, acorde con la estrategia GEL.
Externa	Secretaria de educación	✓ Aumento en los índices de cumplimiento gubernamentales	✓ Informes con los requisitos exigidos según tema.
Externa	Proveedores	✓ Evitar que se conozca la información de transacciones con el Hospital ✓ Realizar acompañamiento frente al cumplimiento de las cláusulas establecidas en los contratos para administrar la información de los clientes del Hospital	✓ asistencia técnica al operador de soporte sobre las políticas de S.I del Hospital. ✓ Garantía de compras.
Externa	Sociedad	✓ Contar con un Hospital que preste servicios de alta calidad. ✓ Encontrar facilidades de acceso al sistema de salud	✓ Cumplimiento de políticas de Seguridad de la Información

Se observa, entre otros aspectos, que la principal preocupación del grupo de interés interno es evitar la pérdida de información que podría originarles repercusiones negativas legales, por lo cual requieren capacitación sobre el tema de asegurar la información por parte de la Institución y de los

entes gubernamentales responsables de brindársela, tales como la alcaldía y los ministerios de salud y tecnología de la información entre otros. Escaso.

6.1.6 Identificación de las Amenazas

Como se ha dejado entrever con anterioridad, los principales activos de información, con dependencia directa, que posee el Hospital San José de Ortega es su base de datos en el SIHOS, respecto a Software, ubicada en su servidor, Hardware, y que se encuentra en la sala de sistemas de la Entidad, Instalación Física, y las cuales al presentar alguna falla en su disponibilidad, confidencialidad y/o integridad explotable por una persona para hackear el sistema, podrían afectar el objetivo principal de esta Empresa Social del Estado conllevando a implicaciones negativas de tipo legal, social y ético, por tanto, se centrarán los siguientes capítulos en el análisis de su actual seguridad.

Prever las diferentes amenazas de tipo informático que eventualmente podrían causar un daño a los activos en su degradación o indisposición total o parcial de sus atributos, es esencial para gestionar el riesgo al cual se pueden ver sometido, siendo uno de los primeros pasos para formular medidas que permitan eliminar, minimizar o transferir el riesgo y que la entidad continúe su actividad normal. Estas amenazas pueden provenir de personas internas o externas a la Entidad por diferentes motivos, como también por fenómenos naturales.

En la siguiente tabla se puede observar las principales amenazas que se ciernen sobre los activos de información en mención:

A= Accidental, D=Deliberada, E= Ambiental

Tabla 7. Principales Amenazas a la Información

TIPO	***AMENAZA***	***ORIGEN***			***VECTOR DE ATAQUE***
		A	***D***	***E***	
Daño Físico	Fuego	X	X	X	❖ Ingresa personal con cigarrillos encendidos. ❖ Equipo entra en corto circuito. ❖ Rompimiento de tubería superior. ❖ Humedad de paredes
	Daños por agua	X	X	X	
	Destrucción del equipo o los medios	X	X	X	
	Polvo, corrosión	X	X	X	
Eventos naturales	Fenómenos climáticos			X	❖ Ingreso de lluvia por techo superior, ventana y/o escaleras contiguas.
	Fenómenos meteorológicos			X	
	Inundación			X	.
Perdida de servicios esenciales	Falla en el aire acondicionado	X			❖ Falencia en el mantenimiento periódico esencial de los dispositivos. ❖ Acceso no protegido a los interruptores de energía.
	Perdida de suministro de energía	X	X	X	
	Falla en el equipo de telecomunicaciones	X	X	X	
Compromiso de la información	Espionaje remoto		X		❖ Ingreso a servidores a través de internet por puertos abiertos, usando exploits. ❖ Ingreso a servidores a través de Red Inalámbrica por puertos abiertos, usando exploits.
	Hurto de medios o documentos		X		
	Hurto de equipos		X		
	Recuperación de medios reciclados		X		
	Divulgación	X	X		

	Datos provenientes de fuentes no confiables	X	X		❖ Ingreso de personas simulando ser paciente con acceso a equipos de oficinas y/o consultorios
	Manipulación con hardware		X		
	Manipulación con software		X		
Fallas técnicas	Falla del equipo	X			❖ Componente entra en sobrecalentamiento por exceso de polvo y/o humedad. ❖ Errores de código que provoca un Bug. ❖ Cantidad de Usuarios mayor a la capacidad de Red.
	Mal funcionamiento del equipo	X			
	Saturación del sistema de información	X			
	Mal funcionamiento del software	X			
	Incumplimiento en el mantenimiento del sistema de información	X			
Acciones no autorizadas	Uso no autorizado del equipo		X		❖ Usuario Administrador instala software no controlado fines personales o laborales.
	Copia fraudulenta del software	X	X		
	Uso de software falso o copiado	X	X		
	Corrupción de los datos	X	X		
	Procesamiento ilegal de los datos		X		
Compromiso de las funciones	Error en el uso	X			❖ Funcionario incapacitado sin remplazo. ❖ Usuario con desconocimiento de utilización de medio.
	Abuso de derechos	X	X		
	Falsificación de derechos		X		
	Negación de acciones	X	X		
	Incumplimiento en la disponibilidad del personal	X	X	X	

Se debe prestar atención principalmente a las fuentes de amenazas que provienen de las personas y cuál sería su motivación para un posible ataque a la estructura informática del Hospital, como se muestra en la siguiente tabla.

Tabla 8. Factores de Amenazas Humanas

FUENTE DE AMENAZA	MOTIVACION	ACCIONES AMENAZANTES
Pirata informático, intruso ilegal	Reto, Ego, Rebelión, Estatus, Dinero	Piratería, Ingeniería Social, Intrusión, accesos forzados al sistema, Acceso no autorizado
Criminal de la computación	Destrucción de la información, Divulgación ilegal de la información, Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador, Acto fraudulento, Soborno de la información Suplantación de identidad, Intrusión en el sistema
Intrusos (Empleados con entrenamiento deficiente, descontentos, malintencionados, negligentes, deshonestos o despedidos)	Curiosidad, Ego, Inteligencia, Ganancia monetaria, Venganza Errores y omisiones no intencionales (ej. Error en el ingreso de datos, error de programación)	Asalto a un empleado, Chantaje, Observar información reservada, Uso inadecuado del computador, fraude, hurto, soborno de información, Ingreso de datos falsos o corruptos, Interceptación, Código malicioso, Venta de información personal, Errores en el sistema, Intrusión al sistema, Sabotaje del sistema, Acceso no autorizado al sistema.

6.1.7 Identificación De Las Vulnerabilidades

Se analizan las diferentes debilidades que posee la Entidad en el ámbito del hardware, software, interfaces de red, controles de acceso y personal, desglosando estos factores y enumerando las posibles amenazas y riesgos, determinando una matriz relacional.

RESPECTO A HARDWARE:

- La Sala de Sistemas no posee una temperatura adecuada.
- En la Sala de Sistemas se presentan descargas estáticas.
- No existe un sistema de detección de incendios.
- No existe un inventario de Hardware actualizado.
- No existe un inventario de Software actualizado.
- Es necesario la migración (actualización) del hardware en la mayoría de los equipos, sobre todo en aquellos que intervienen en la atención al público.

RESPECTO A SISTEMA DE INFORMACIÓN:

- No se almacenan adecuadamente las copias de respaldo.
- Las actualizaciones no se instalan según necesidades.
- No existe un antivirus Corporativo.
- No hay implementado un IDS o IPS.

- No se realiza borrado seguro a dispositivos en devolución.
- Existen equipos con software no autorizado.
- No hay debidamente definidos perfiles de usuarios en los equipos.
- No se tiene debidamente identificada y clasificada la información según su nivel de importancia.
- No existe un documento de adaptabilidad de políticas de S.I. en la institución.
- No existe un acuerdo de confidencialidad en cuanto a la información que se accede.
- No existe un canal y procedimientos claros a seguir en caso de incidente de seguridad.

RESPECTO A LA RED DE DATOS:

- Todos los equipos no se encuentran dentro de la red.
- No hay un dominio de red de trabajo creado.
- La red no está segmentada (VLAN).
- No se cuentan con firewall físicos instalados y configurados para la red LAN y salida a internet.

RESPECTO A CONTROL DE ACCESO:

- Sala de Sistemas no cuenta con los controles necesarios de acceso.
- No existe un sistema de vigilancia electrónico.

- Las contraseñas para ingreso al Sistema no cumplen requisitos.
- No se controla el acceso a sitios web.
- No se controla el acceso a Correo electrónico.
- No se ha diseñado e implementado ACL
- No se controla y restringe el uso y la asignación de privilegios de acceso.

RESPECTO A PERSONAL:

- No hay capacitación apropiada a los usuarios de los sistemas.
- No hay suficiente personal de informática.
- No hay personal capacitado para tratamiento de Incidentes informáticos.
- Falta personal de vigilancia

Tabla 9. Matriz Factores de Riesgo Hardware

Clasificación	*Vulnerabilidad*	*Causa*	*Amenaza*	*Riesgos*
Hardware	La Sala de Sistemas no posee una temperatura adecuada.	El aire acondicionado no tiene la capacidad suficiente de enfriamiento	Cambio imprevisible en el medio ambiente.	Perdida de Componentes del Sistema por Alta Temperatura.
	En la Sala de Sistemas se presentan descargas estáticas.	No cuenta con piso falso o aislante.	El Personal ingresa con carga electrostática.	Daño en dispositivos electrónicos.
	No existe un sistema de detección de incendios.	Falta de planeación en la ejecución presupuestal.	Se presenta una conflagración en las instalaciones.	Pérdidas de Vidas Humanas y/o equipos de computo
	No existe un inventario de hardware actualizado.	Sin Tiempo el Técnico y equipos fuera de red.	Caídas del Sistema (Las aplicaciones exigen más hardware del instalado)	Lentitud de los servicios Misionales y Administrativos.
	No existe un inventario de Software actualizado	La falta de implementación políticas de seguridad informática	No se sabe con exactitud el software instalados en los equipos de computo	La mala prestación de los servicios misionales y desarrollo de actividades administrativas
	Es necesaria la migración (Actualización) del hardware en la mayoría de los equipos, sobre todo en aquellos que intervienen en la atención al público.	No se ha dado la organización e importancia al recurso tecnológico de la entidad	El nuevo software adquirido no funciona en los equipos dispuestos	El no uso de las herramientas más idóneas dispuesta para la realización de las labores

Tabla 10. Matriz Factores de Riesgo Sistemas de Información

Clasificación	*Vulnerabilidad*	*Causa*	*Amenaza*	*Riesgos*
Sistemas de Información	No se tiene automatizado y debidamente implementado Políticas de seguridad para la administración de backup.	Falta de adopción de políticas de seguridad informática en la institución	Daños en el dispositivo donde se encuentra la información almacenada	Perdida de información
	No se almacenan adecuadamente las copias de respaldo.	No se cuenta con discos duros para almacenamiento independiente.	Perdida de información en producción.	Parálisis en la ejecución de tareas sistematizadas.
	Las actualizaciones no se instalan según necesidades.	Equipos fuera de red – falta gestión informática	Ataque por parte de delincuentes informáticos.	Perdida o fuga Información
	No existe un antivirus Corporativo.	Falta de planeación en la ejecución presupuestal	Instalación de Software Malicioso.	Perdida o fuga Información
	No hay implementado un IDS o IPS.	Falta de Conocimiento de la persona a cargo	Ingreso de hackers Modificación de Archivos del Sistema.	Perdida o fuga Información
	No se realiza borrado seguro a dispositivos en devolución.	Falta de Conocimiento de la persona a cargo	Personas externas acceden a los dispositivos de almacenamiento.	Fuga de información misional.
	Existen equipos con software no autorizado.	Equipos fuera de red- configuración políticas de seguridad	Ingreso de código malicioso al sistema	Pérdida, fuga o indisponibilidad del sistema.
	No existe un inventario de software actualizado.	Sin Tiempo el Técnico y equipos fuera de red.	Visita de Organismos de Control	Se presentan sanciones penales y administrativas contra la Entidad.
	No hay debidamente definidos perfiles de usuarios en los equipos.	Falta de adopción de políticas de seguridad informática en la institución	Todos los usuarios modifican las configuraciones	Daño del sistema operativo, la perdida de integridad del sistema

Tabla 11. Matriz Factores de Riesgo Sistemas de Información y Red

Clasificación	*Vulnerabilidad*	*Causa*	*Amenaza*	*Riesgos*
Sistemas de Información	No se tiene debidamente identificada y clasificada la Información según su nivel de importancia.	Falta de Gestión de Gobierno de TI en la entidad	Uso y filtración de la documentación critica de la entidad.	Perdida de información
	No existe un documento de adaptabilidad de políticas de S.I. en la institución.	Desconocimiento de los fundamentos de S.I.	No uso de políticas claras para el manejo y aplicación de la S.I.	Acceso a la información por parte de terceros.
	No existe un acuerdo de confidencialidad en cuanto a la información que se accede.	Falta de definición de procesos y procedimientos, o manual de funciones a través de procesos	Manipulación y filtración de información a personal no autorizado.	Interpretación inadecuada de información confidencial
	No existe un canal y procedimientos claros a seguir en caso de incidente de seguridad.	Falta de definición de procesos y procedimientos, o manual de funciones a través de procesos	Presentación de incidentes, ataque, perdida de información	No disponibilidad de la información y servicios.
Red	Todos los equipos no se encuentran dentro de la red.	Falta de planeación en la ejecución presupuestal.	Ausencia de reglas en los Equipos.	Usuarios no dedican todo el tiempo a labor misional
	La red no está segmentada (VLAN).	Falta de Conocimiento de la persona a cargo- Falta de planeación en la ejecución presupuestal.	Personal accede a documentos no autorizados	Fuga de información misional.
	No se cuentan con firewall físicos instalados y configurados para la red LAN y salida a internet.	Falta de planeación en la ejecución presupuestal.	Acceso de entidades no autorizadas-virus etc.	Alteración en configuración de la red.

Tabla 12. Matriz Factores de Riesgo Control de Acceso

Clasificación	*Vulnerabilidad*	*Causa*	*Amenaza*	*Riesgos*

Control de Acceso	La Sala de Sistemas no cuenta con los controles necesarios de acceso.	Falta de planeación en la ejecución presupuestal	Personal no autorizado dispone de dispositivos	Avería o perdida de elementos informáticos
	No existe un sistema de vigilancia electrónico.	Falta de planeación en la ejecución presupuestal	Personas ingresa a Sistemas de Información	Avería o perdida de elementos informáticos
	Las contraseñas para ingreso al Sistema no cumplen requisitos.	Mala configuración de políticas de seguridad	Personas acceden a datos confidenciales	Fuga de información.
	No se controla el acceso a sitios web.	Falta de Conocimiento de la persona a cargo	Usuario gasta recursos del sistema	Lentitud de los servicios Misionales y Administrativos
	No se controla el acceso a Correo electrónico.	Falta de Conocimiento de la persona a cargo	Usuario instala, inconscientemente, Software Malicioso	Fuga de información
	No se ha diseñado e implementado ACL	Falta de Conocimiento de la persona a cargo	Hackers Ingresan a la Red Interna.	Fuga de información
	No se controla y restringe el uso y la asignación de privilegios de acceso	Falta de implementación de herramientas de control de acceso tanto físico como a nivel de red.	Libre movimiento de personas dentro del área y libre acceso a los recursos de red.	Pérdida o alteración de la información tanto a nivel físico como a nivel lógico.

6.1.7.1 Pruebas de Vulnerabilidad.

Con el fin de determinar cuan vulnerable son los activos esenciales de información del Hospital se procede a realizar evaluación técnica, para lo cual se opta ejecutarla como una prueba con conocimiento nulo del entorno, que está definida como un simulacro de un ataque real, sin que se tenga un conocimiento de la composición física o lógica de la entidad objetivo.

Vale la pena hacer la salvedad que el trabajo no está centrado en la Gestión del Riegos específicamente, por lo cual este punto se toma como una "Proof of Concept" porque se quiere demostrar, que lo que se halle, podría ser explotado de una manera útil para el intruso, sin hacer exhaustivo su procedimiento.

Alcance.

El alcance de la evaluación a realizar esta delimitado por los aspectos señalados en la siguiente tabla:

Tabla 13. Delimitación pruebas de vulnerabilidad

Responsable	***Tiempo***	***Sistemas Involucrados- Objetivo***	***Posibles Incidente Provocados***	***Herramientas Utilizadas- Atacante***
Héctor Ricardo Triana Acevedo	Dos domingos/ Dos sábados	❖ Red WIFI ❖ IP Publica	Denegación del Servicio	❖ Un Portátil ❖ Memorias USB con Wifislax y Parrot OS

Procedimiento.

Para la realización de evaluación técnica de vulnerabilidades en el Hospital de Ortega se observa el procedimiento descrito por el Ministerio de Comunicaciones, reflejado en la figura 20 de donde se abarcarán las cinco primeras fases:

Figura 20. Ciclo para la Ejecución de Pruebas de Efectividad Técnicas
Adaptado de la Guía Pruebas de Efectividad, MINTIC. (2016). Tomado de https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

Contextualización.

Se definen el alcance específico de las pruebas a realizar para lo cual se tiene en cuenta:

- Objetivos Para Evaluar: Seguridad WIFI; Seguridad en el servidor de que contiene el SIHOS.
- Objetivo Corporativo Especifico: Conocer vulnerabilidades y vectores de ataque.
- Horario: Fines de semana, Domingo ataque WAN, por cuanto se busca acceso a través de dirección IP publica, sin importar conexiones; sábado, ataque LAN, se requiere conexiones activas para el éxito de la labor y se encuentra la mayoría de personal laborando en horas de la mañana. No se realiza entre semana por cuanto los clientes del Hospital acuden masivamente en ese horario, en especial los pacientes médicos y podrían verse afectados por una eventual caída del servicio.
- Direcciones IP Objetivo: Interna 192.168.2.2, Externa 190.90.X.X
- Acciones Posteriores a Acceso: al ingresar remotamente al servidor SIHOS, se buscará colocar un archivo de texto plano en su directorio raíz, si es Linux, o bien, si Windows en C: lo cual demostraría que se tiene permisos root o de administrador, según el caso, evidenciando que se podría realizar tareas elevadas en el servidor, como copiar, borrar, modificar y/o ejecutar.
- Uso Ingeniería Social: Si, en su primera fase se podría utilizar para tratar de conocer la IP externa del servidor, aprovechando que la mayoría de los usuarios

atienden publico indiscriminadamente, si no es posible, se intentará con una herramienta de software.

Reconocimiento.

Para tratar de identificar la IP externa del servidor se utiliza, en primera instancia la técnica del Ingeniería Social Shoulder Surfing, para lo cual se realiza un recorrido por las instalaciones en búsqueda de un usuario ingresando o dentro del sistema SIHOS y efectivamente se ubica a uno de los funcionarios que se encuentra en el sistema objetivo a través de su IP publica, observable en el espacio URL sin ningún enmascaramiento lo cual podría representar en sí una vulnerabilidad explotable. En la figura 21 se muestra la captura de pantalla reseñada:

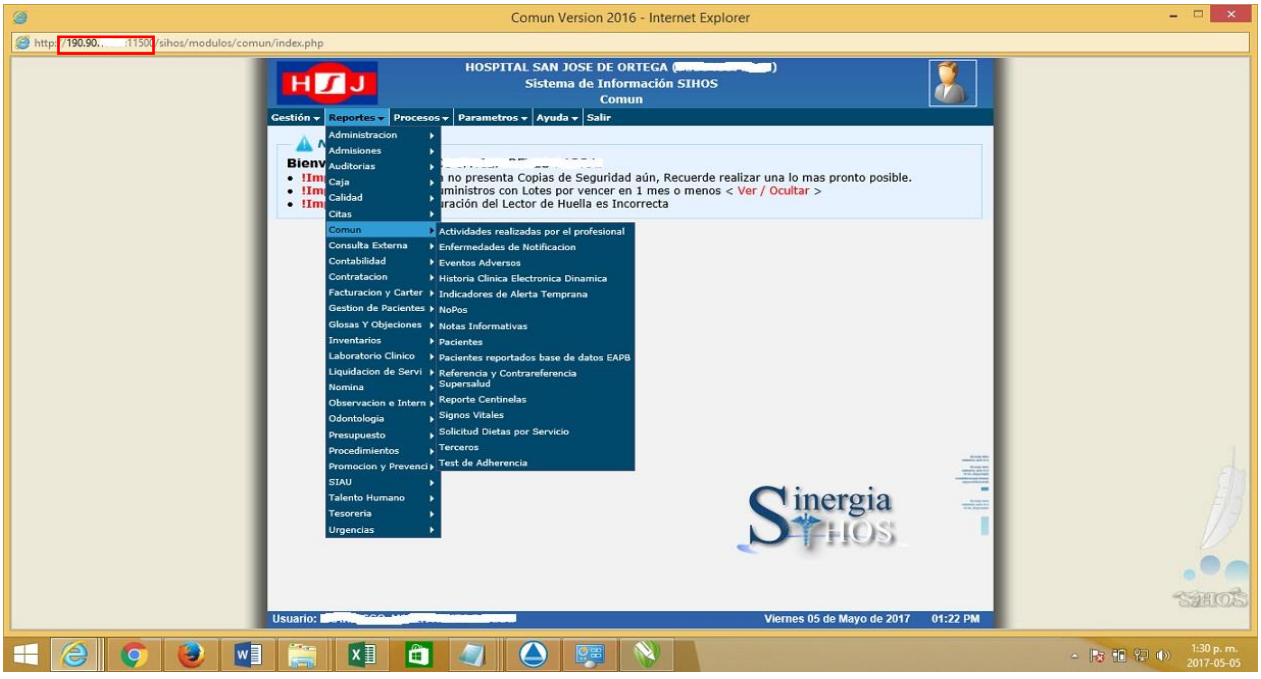


Figura 21. Ventana con IP Servidor a la Vista

Modelado de amenazas.

Se vislumbra el interés que podría tener un atacante en vulnerar el activo de información que para el caso concreto de estudio es el SIHOS de la Entidad, desde dos perspectivas:

- Punto de Vista de la Entidad: Se trata de entender que sucedería si se vulnerara la confidencialidad de los activos analizados, que probabilidad existe de ellos suceda y que repercusión tendría la divulgación.

  Para esto se debe tener en cuenta que la base de datos del SIHOS según los módulos de información que posee, contiene datos financieros, de los funcionarios de la entidad, de los pacientes y de los proveedores, por cuanto es una base unificada de información, por lo cual al obtener acceso a sus tablas vulneraria datos de varios frentes.

  Y aunque en un principio se piense que un atacante no tendría interés en este activo especifico, por ser un hospital con el nivel más bajo, uno, aunado a esto, la población que atiende es de bajos recursos, vale la pena analizar que la divulgación no autorizada de las historias clínicas podría traer graves repercusiones de tipo legal y financiero a la Entidad.

  Así mismo, el eventual cifrado del historial clínico de los pacientes por parte de un atacante podría obligar al hospital al "pago de un rescate" de la información. También y como ya se ha mencionado antes, existen datos financieros que podrían

servir de plataforma a un posterior ataque a las transacciones bancarias en línea que realiza el Hospital.

- Punto de Vista del Atacante: Se identifican cuáles serían los grupos de personas que podrían interesarse en atentar contra los atributos de la información de los activos analizados, los cuales se reflejan en la siguiente tabla:

Tabla 14. Posibles Grupos Atacantes contra Activos de Información

INTERNOS	***EXTERNOS***
Empleados	Contratistas
	Crimen Organizado
Contratistas	Script Kiddies
	exempleados
	Proveedores

El grupo que representan un mayor riesgo serían los empleados por cuanto pueden presentar doble motivación, venganza y/o retribución económica, además, tiene un mayor conocimiento para lograr accesibilidad lógica o físico al activo objetivo.

Análisis de vulnerabilidades.

Como se menciona en el punto anterior la principal amenaza que se cierne sobre el Hospital serían sus mismos empleados o exempleados, que, por lo general, no tienen

conocimientos avanzados sobre informática, por tanto, debe simularse un ataque que se pueda llevar acabo con herramientas del ciberespacio y documentación a la mano, como la existente en la web, por ejemplo, en los canales de YouTube. Asimismo, no se utilizan técnicas o herramientas para anonimizar la incursión informática, por ser una Prueba de Concepto.

Teniendo la dirección de IP Publica del Servidor objetivos planea, en primera instancia, un ataque WAN, para lo que se efectúa una verificación preliminar, activa y automatizada del mismo a través de la herramienta NMAP, contenida en la distribución de Linux, Parrot OS o Wifislax, entre otros, la cual permite conocer que puertos tiene abiertos, utilizando su comando básico "nmap 190.90.X.X" como se observa en la figura 22:

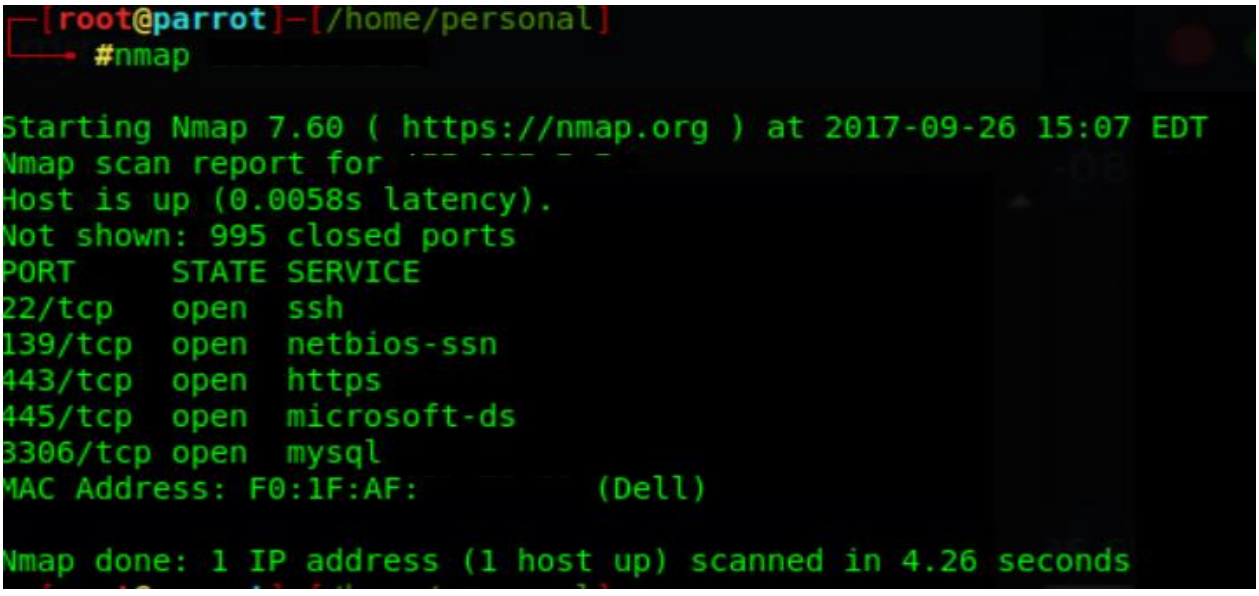


Figura 22. Escaneo con Nmap

El servidor en cuestión tiene cuatro puertos abiertos, 22(SSH), 139(NETBIOS), 443 (HTTPS) y 3306 (MYSQL), por los cuales se va a tratar de tener acceso al sistema, por cuanto existen exploits específicos que aprovechan ciertas vulnerabilidades en estos servicios.

Explotación.

Para esta fase se utiliza una herramienta también, de Parrot OS, totalmente automatizada y que por lo cual no requiere conocimientos avanzados, como tampoco, mucho esfuerzo denominada ARMITAGE, la cual es una interfaz gráfica del proyecto Metasploit, desde donde se pueden ejecutar exploits para los servicios encontrados, pero teniendo en cuenta que se busca demostrar el ataque puede ser llevado a cabo sin conocimientos avanzados en pruebas de explotación, se utiliza la "Hail Mary" que hace que la herramienta haga una búsqueda automática de exploit para el objetivo específico y la ejecuta y como se puede observar en la figura 23, logra ingresar al objetivo, a través del puerto 136, exploit para samba "is_know_pipename".

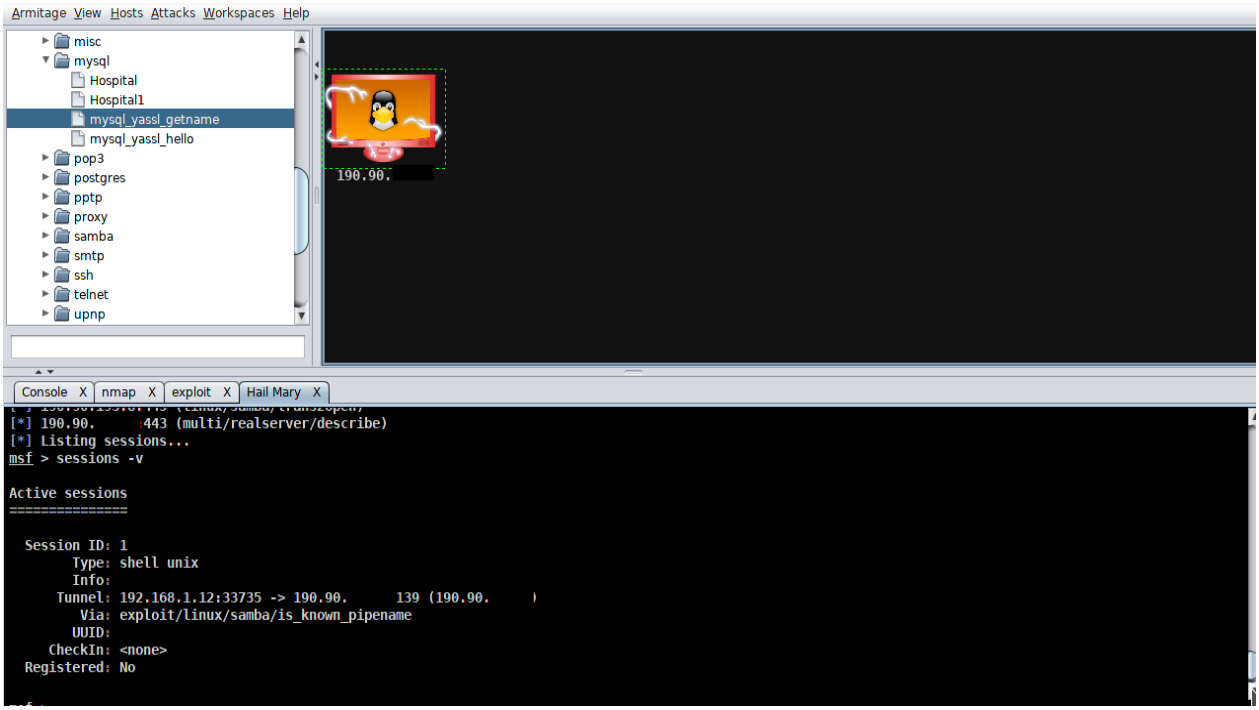


Figura 23. Usando Hail Mary en Armitage

Se obtiene una Shell root lo cual nos permite realizar cualquier modificación en el sistema, se navega hasta la ruta donde se encuentra la base de datos del SIHOS, como se muestra en la figura 24, la cual se podría borrar, copiar, denegar su servicio, o bien cambiar la clave root de MySQL, para ingresar directamente a la base de datos.

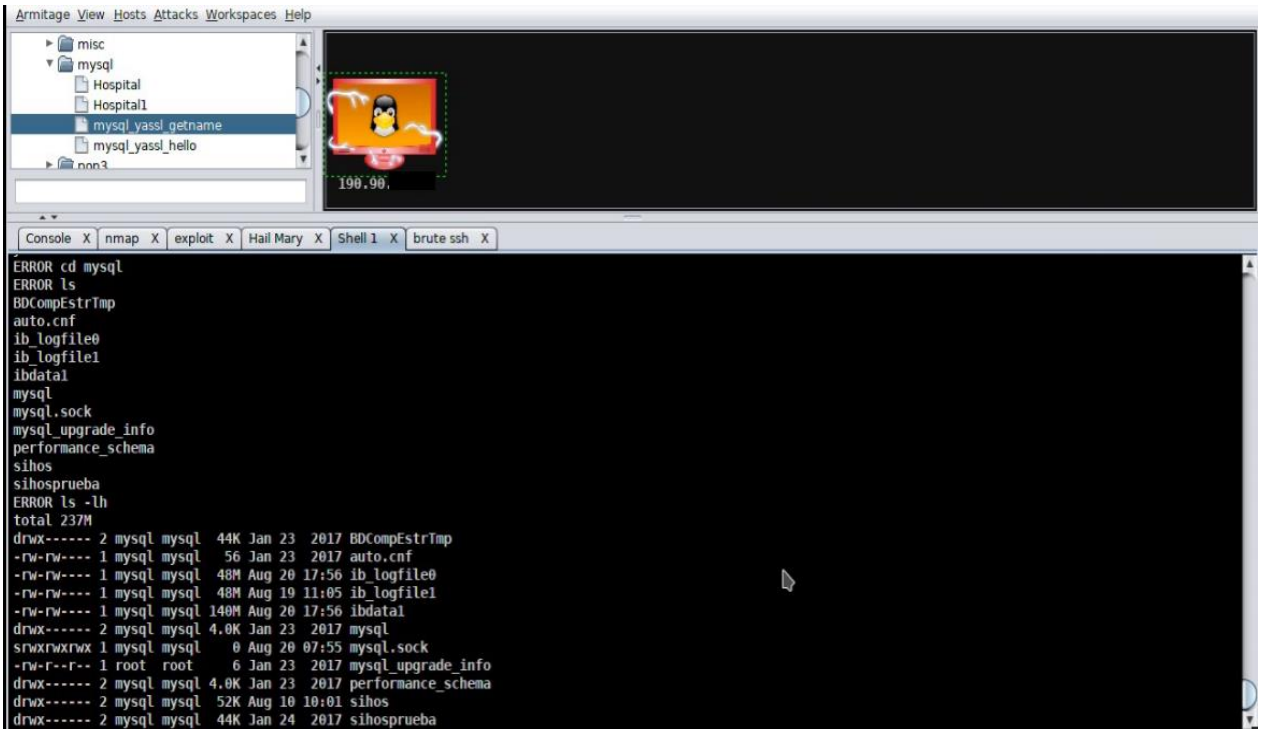


Figura 24. Ruta SIHOS en Armitage

6.1.7.1.1 Otros ataques.

Aunque ya se logra el objetivo primario que es lograr el acceso como root al servidor que contiene la base de datos SIHOS desde cualquier lugar, se realizan otras pruebas para establecer otras debilidades de la infraestructura tecnológica actual.

WLAN.

Se utiliza la herramienta fluxión (podría ser también LINSET, que cumple el mismo objetivo), previamente instalada en la distribución Parrot OS, la cual hace uso de nmap para localizar redes wifi, para posteriormente realizar una desautenticación a un router especificado con el fin de obtener su handshake, una vez logrado este paso suplanta el router objetivo colocándose a la escucha de un host que quiera conectarse, como se observa en la figura 25:

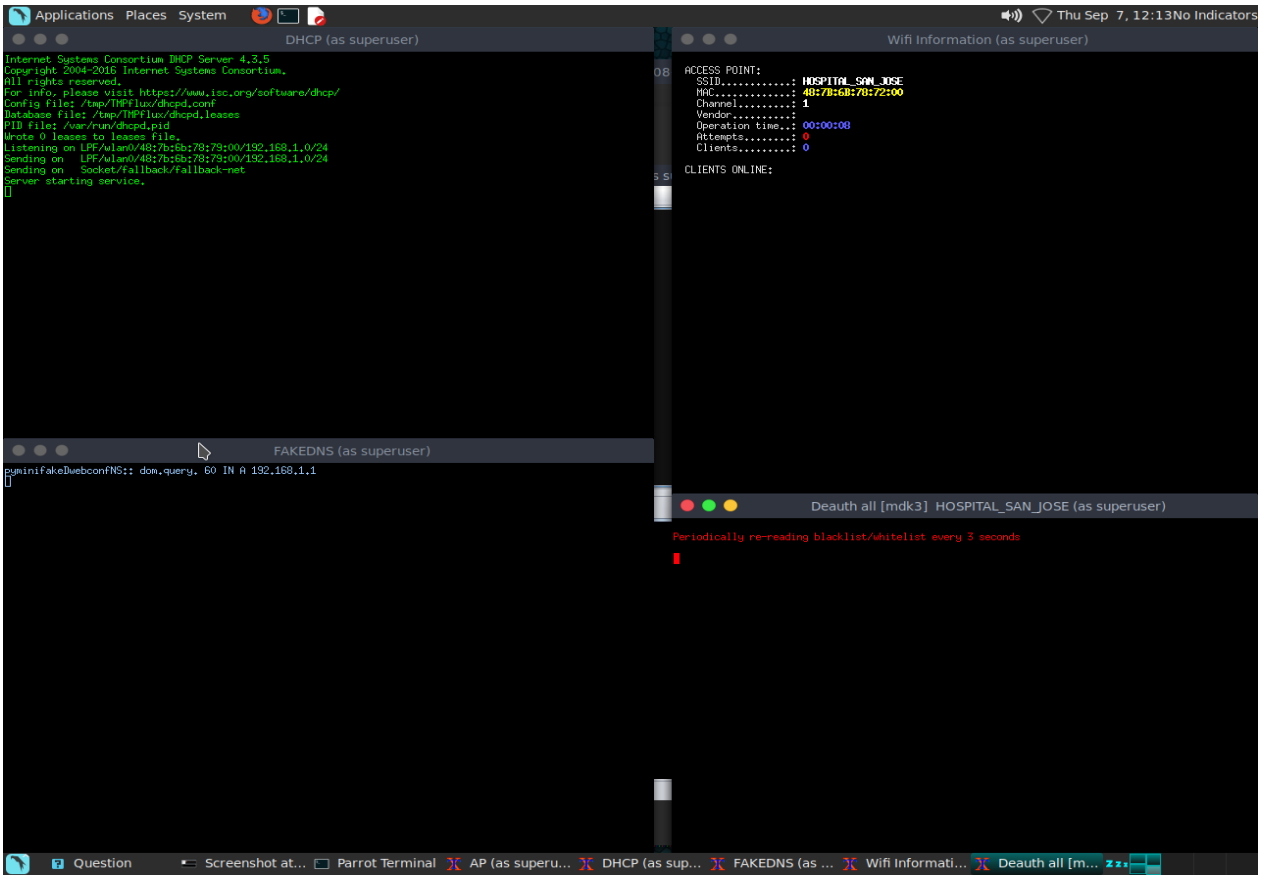


Figura 25. Herramienta Fluxión a la Escucha

Si se conecta un cliente le solicita la contraseña, la cual compara con el handshake previamente capturado, como se observa en la figura 26:

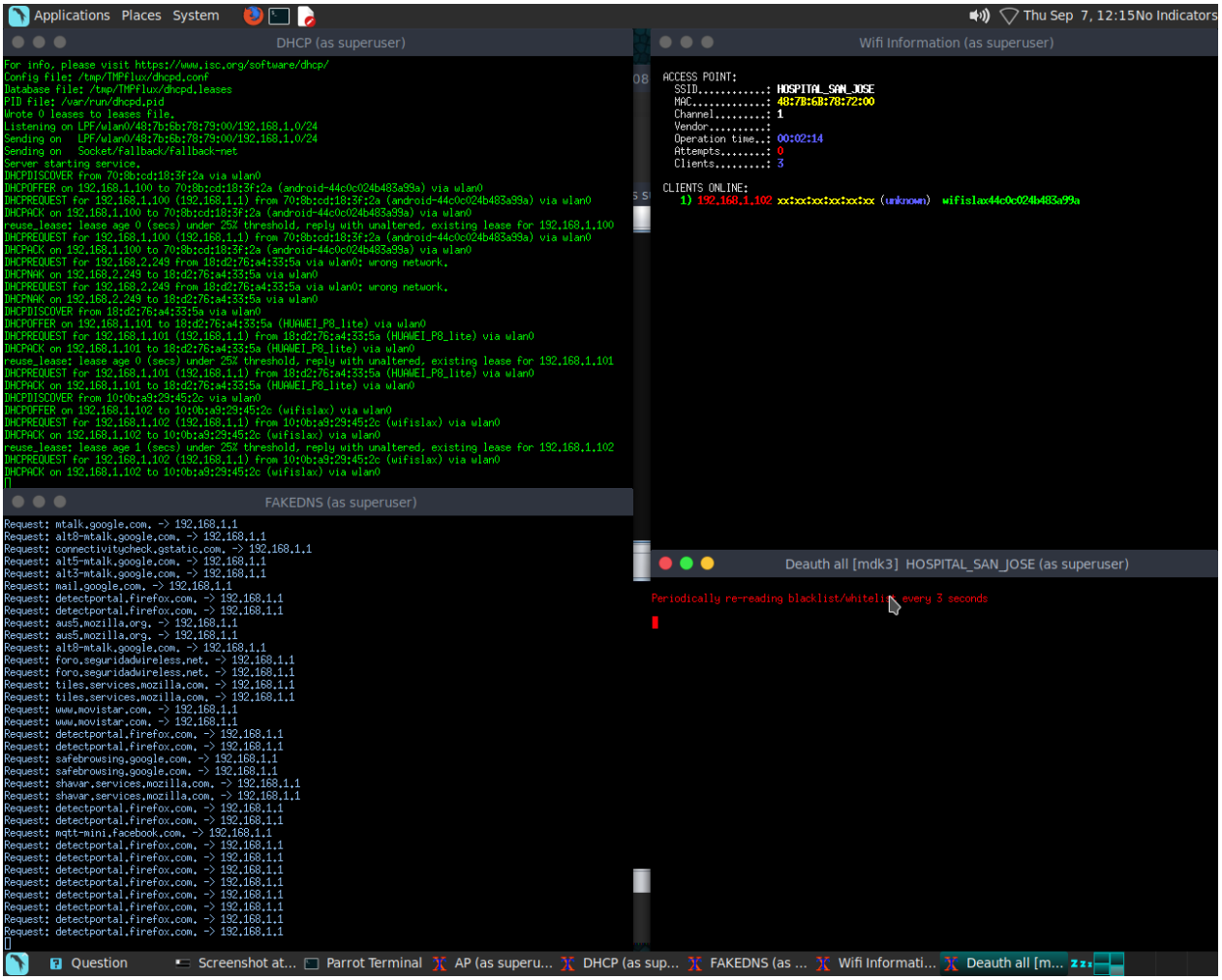


Figura 26. Herramienta Fluxión Cliente Conectado

Para posteriormente y una vez comparado con el uso de aicrack-ng, procede a indicar la contraseña de ingreso a la red local, como se observa en la figura 27:

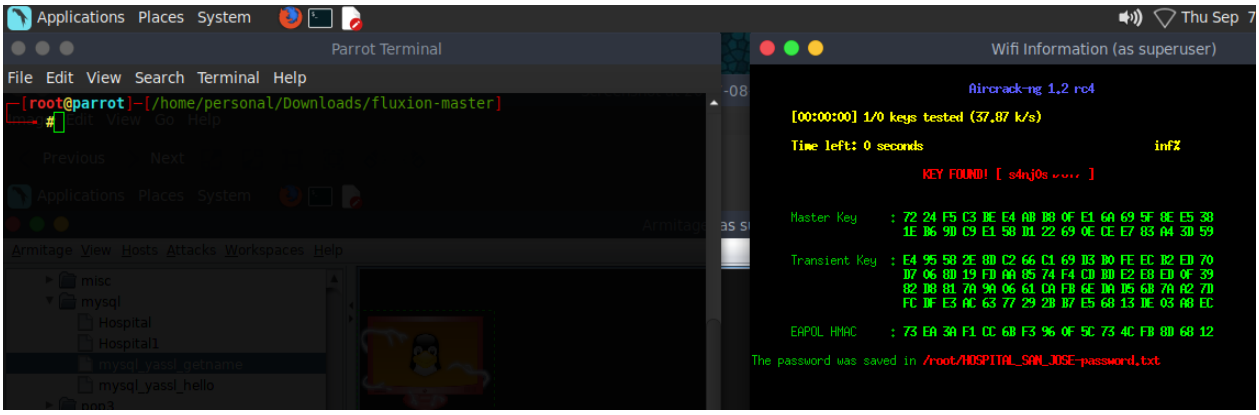


Figura 27. Herramienta Fluxión Halla contraseña

Una vez se obtiene acceso a la red local se puede realizar ataques más efectivos como Man In The Middle, MITM, por tal motivo se usa la herramienta A2SV de Parrot OS, que busca vulnerabilidades SSL automáticamente, contra el servidor de SIHOS, obteniendo como resultado que el servidor puede ser vulnerable al ataque de CRIME (SDPY) y SSLv3 POODLE, como se detalla en la figura 28:

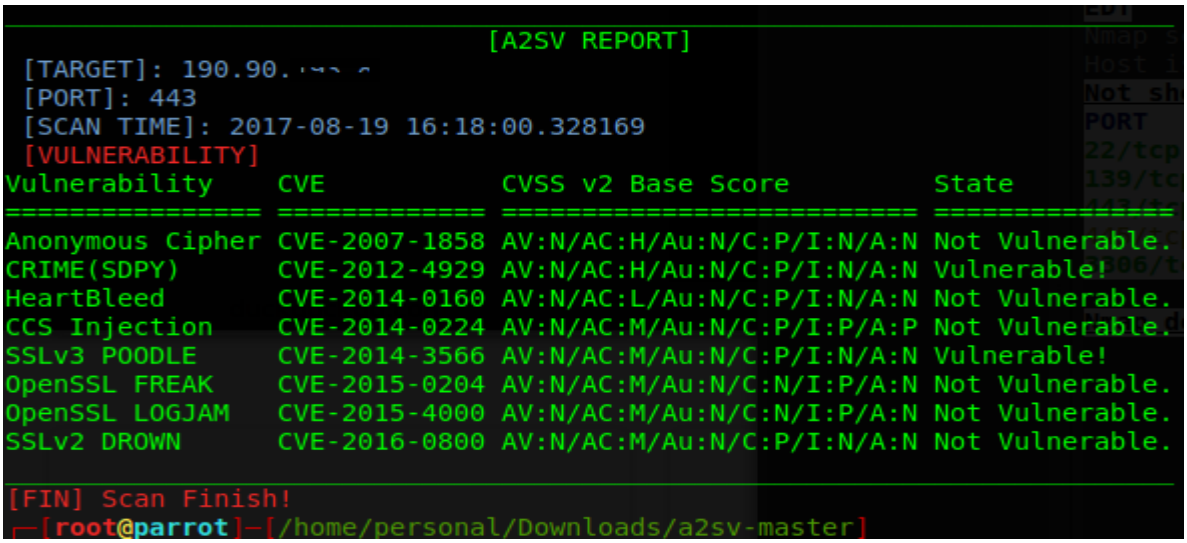


Figura 28. Herramienta A2SV Report

6.1.8 Matriz DOFA

Realizadas las anteriores actividades se determina la influencia de ciertos elementos y como inciden en la planeación y posterior implementación del MSPI en esta Empresa Social del Estado, los cuales se relacionan en la siguiente Matriz DOFA:

Tabla 15. Matriz DOFA

DOFA Hospital San José de Ortega (MSPI)	***Fortaleza***	***Debilidad***
	✓ Disposición positiva de la gerencia para la ejecución del Modelo de Seguridad y Privacidad de la Información en el Hospital	✓ Personal con escaso conocimiento sobre temas relacionados con la seguridad de la información y nuevas tecnologías ✓ Insuficiente tiempo por parte de los funcionarios para establecer las debilidades y necesidades de los procesos misionales y de apoyo ✓ Infraestructura física y tecnológica insuficiente para cambios u optimización de procesos de TI
Oportunidad	***Estrategia FO***	***Estrategia DO***
✓ Apoyo del MINTIC en capacitación y programas relacionados con GEL. ✓ Capacitación virtual accesible a los funcionarios como ciudadano digital	✓ Gestionar con las Directivas espacios para capacitación en temas de TIC	✓ Mejorar las competencias laborales de los empleados respecto a las TIC
Amenaza	***Estrategia FA***	***Estrategia DA***
✓ Incremento de los ciberataques	✓ Fortalecer los conocimientos técnicos del encargado del área informática con el fin de evitar y/o minimizar el riego que una amenaza impacte negativamente un activo	✓ Adoptar un Modelo de Gestión de la Seguridad de la Información en la Entidad.

✓ Limitado presupuesto para implantación de nuevas tecnologías	✓ Incluir en los planes administrativos del Hospital la compra de equipos necesarios para asegurar la red informática

Se puede concluir que la mayor barrera que se tiene para ejecución del MSPI es la falta de presupuesto que se asigna a tecnología, en especial a temas relacionados con seguridad de la información, agregando esto el escaso tiempo que pueden dedicar los funcionarios a este tema en particular, pero se cuenta con el aval de la alta dirección y el apoyo educativo del MINTIC, para eventualmente capacitar a los funcionarios en temas de las TIC, siendo fundamental teniendo en cuenta que como siempre se ha mencionado el eslabón más débil en la cadena de seguridad es el personal y no la tecnología que usan.

6.1.9 Resultado Etapa de Diagnóstico

Una vez ejecutada la fase de diagnóstico se realiza un diagrama de las capacidades relacionadas con el tema de la seguridad de la información en los principales aspectos evidenciados en el hospital san José de Ortega con base en el personal, procesos y herramientas, enmarcando un estado en escala de 1 a 5 de grado de madurez, como se observa en la figura 29:

Capacidad	1 No capacidad	2 Capacidad aislada	3 Capacidad sirviendo	4 Capacidad estratégica	5 Capacidad diferenciada
Formación a todo el Personal sobre Adopción de Políticas y Procedimientos de S.I	No existe entrenamiento alguno	Adquieren formación general por internet	Sensibilizaciones elementales en S.I	Capacitación sobre el MSPI	Capacitaciones evaluadas sobre MSPI
Capacitación al Encargado del Proceso de Gestión de T.I en temas de Ciberseguridad	No existe Capación sobre el tema	Se capacita por sí mismo	Asistencia a talleres y charlas de MSPI	Capacitación Configuración dispositivos S.I	Posgrado en ciberseguridad
Optimización de las TIC en los procesos Gestión, Misional y de Apoyo	No existe mejoramiento alguno	Mejoras esporádicas no planificadas	Se da cumplimento al PETI	Cumplimiento estricto del PETI	Mejora continua
Ejecución de recursos financieros asignado al proceso estratégico a S.I	No se han realizado compras para S.I	Se realiza gestión compra equipos/licencias	Se adquiere servidor de dominio	Se adquiere UTM	Se cuenta con todas las licencias S.I
Minimización del Riesgo Informático por Exposición Interna y Externa	Nunca se ha reducido el Riesgo en S.I	Mejoras esporádicas no planificadas	Se configura apropiadamente UTM	Actualizaciones periódicas de reglas y seguimiento	Mejora continua
Control de Usuarios y Dispositivos en la Red Informática	No existe control en la red informática	Se realiza en situ eventualmente	Se configura apropiadamente active directory	Actualizaciones periódicas de reglas y seguimiento	Mejora continua

Figura 29. Escala Estado de Madurez S.I

Con base en la información de la figura anterior y los datos recolectados durante esta fase, el estado actual del Hospital San José de Ortega es el que se observa en la figura 30:

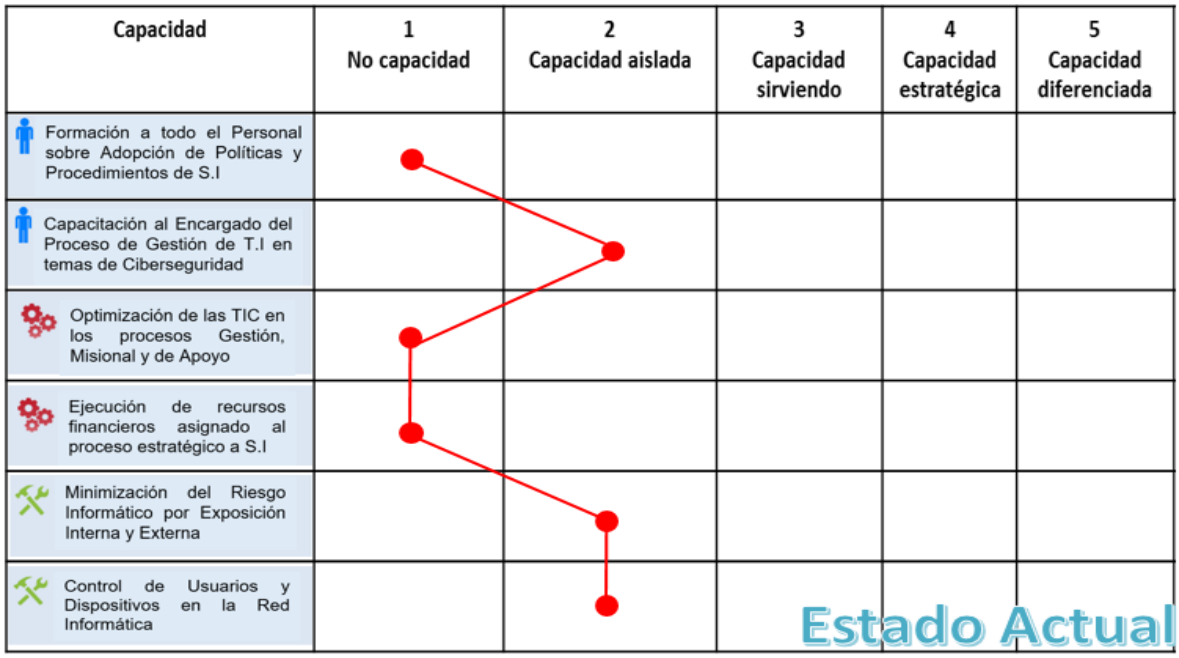


Figura 30. Diagrama AS-IS de S.I, Fase de Diagnóstico

Como se observa el Hospital no cuenta con personal capacitado en seguridad de la información, consecuencia directa de no tener políticas y procedimientos de seguridad. El encargado del área de informática no posee capacitaciones especificas en el área de la seguridad de la información. Tampoco se ha ido mejorando los procesos inherentes a las tecnologías de la información que impactan de forma negativa el ámbito de la seguridad, por lo cual se hace necesario se le dé aplicabilidad al Plan Estratégico de Tecnología de la Información, PETI.

No se han gestionado recursos ante la junta directiva para la compra de dispositivos y licencias que permitan asegurar los datos personales contenidos en los diferentes dispositivos y que circulan por la red para reducir el riesgo de pérdida o indisponibilidad de la información y tener un control centralizado de los usuarios, computadores, smartphones, puntos de acceso que se encuentran en todas las dependencias institucionales.

6.2 Desarrollo Fase De Planeación

Obtenida la información de la etapa de diagnóstico se procede a ejecutar la fase de planeación, según las necesidades observadas y datos recolectados que permitan cerrar la brecha que presenta en el tema de seguridad de la información en el Hospital.

6.2.1 Políticas De Seguridad De La Información

6.2.1.1 General.

El Hospital San José de Ortega no cuenta con una política general de información por lo cual se propone el siguiente documento, acorde con los lineamientos del Ministerio de las Comunicaciones, según la Estrategia de Gobierno en Línea:

La dirección del HOSPITAL SAN JOSE DE ORTEGA, TOLIMA, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la entidad.

Para el HOSPITAL SAN JOSE DE ORTEGA, TOLIMA, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Entidad según como se defina en el alcance, sus funcionarios, terceros, aprendices, practicantes, proveedores y la ciudadanía en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del HOSPITAL SAN JOSE DE ORTEGA, TOLIMA
- Garantizar la continuidad del negocio frente a incidentes.
- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA ha decidido **definir, implementar, operar y mejorar** de forma continua un Sistema de Gestión de

Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.

6.2.1.1.1 Principios de seguridad.

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA protegerá su información de las amenazas originadas por parte del personal.

- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA implementará control de acceso a la información, sistemas y recursos de red.
- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.
- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- EL HOSPITAL SAN JOSE DE ORTEGA, TOLIMA garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

El incumplimiento a la política de Seguridad y Privacidad de la Información traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo

establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere. (Guía Elaboración de la política general de seguridad y privacidad de la información MINTIC, 2016)

6.2.1.2 Especifica.

6.2.1.2.1 Organización.

- El comité de seguridad de la Información está conformado por el gerente y el jefe de cada una de las dependencias del Hospital. El Comité tendrá los siguientes objetivos:
- Revisar y proponer a la Junta directiva para su consideración y posterior aprobación, las políticas de seguridad de la información y las funciones generales en materia de seguridad de la información que fuera convenientes y apropiadas para el Hospital.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de la información de este Hospital frente a posibles amenazas, sean internas o externas.
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes, relativos a la seguridad, que se produzcan en el ámbito de este Hospital.
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo con las competencias y responsabilidades asignadas a cada sector, así

como acordar y aprobar metodologías y procesos específicos relativos a la seguridad de la información

- Evaluar y coordinar la implementación de controles específicos de seguridad se la información para los sistemas o servicios de este Hospital, sean preexistente o nuevos.
- Promover la difusión y apoyo a la seguridad de la información dentro del Hospital, como así, coordinar el proceso de administración de la continuidad de las actividades.

6.2.1.2.2 Gestión de activos.

- Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.
- El mismo será actualizado ante cualquier modificación de la información registrada y revisado con una periodicidad no mayor a 6 meses.
- El encargado de elaborar el inventario y mantenerlo actualizado es cada Responsable de Unidad Organizativa.
- Para clasificar un Activo de Información, se evaluarán las tres características de la información en las cuales se basa la seguridad, confidencialidad, integridad y disponibilidad.
- Se definirán procedimientos para el rotulado y manejo de información, de acuerdo con el esquema de clasificación definido. Los mismos contemplarán los recursos de

información tanto en formatos físicos como electrónicos e incorporarán las siguientes actividades de procesamiento de la información, copia, almacenamiento, transmisión por correo, fax, correo electrónico, transmisión oral.

6.2.1.2.3 Control de acceso.

- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran área de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico en el perímetro tales que puedan ser auditadas, así como con procedimientos de seguridad operacionales que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

- Cuando se requiere el soporte técnico o mantenimiento de equipos de infraestructura tecnológica dentro de las Instalaciones debe diligenciar el Formato de Autorización de Soporte Técnico, previo visto bueno del área usuaria y El Administrador o quien haga sus veces.

- Toda contraseña asignada para acceder al sistema de información o equipo de cómputo deberá ser asignada de manera individual, y cada usuario deberá mantenerla

de manera confidencial y queda prohibido divulgarla o prestarla; el usuario como encargado del tratamiento de datos es responsable disciplinaria, administrativa y penalmente, según sea el caso, por el acceso inusual a los recursos informáticos que sean realizados con su usuario y contraseña.

- En ninguna circunstancia los equipos de cómputo pueden ser dejados desatendidos en lugares públicos o a la vista, en el caso que esté siendo transportado en un vehículo.

- Los equipos de infraestructura de la E.S.E. Hospital San José de Ortega, deben ser transportados con las medidas de seguridad apropiadas, que garanticen la integridad física de los dispositivos.

- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.
- Los equipos de la E.S.E. Hospital San Rafael Tunja deberán contar con un seguro que los proteja de robo.

- En caso de pérdida o robo de un equipo de la E.S.E. Hospital San José de Ortega, se deberá informar inmediatamente al correo electrónico: sistemas@hospitalsanjoseortega.gov.co, para que se inicie el trámite interno y se deberá poner la denuncia ante la autoridad competente.

- El retiro de equipos de cómputo, periféricos, dispositivos de almacenamientos, software e información considerada crítica propiedad de la E.S.E. Hospital San José de Ortega, fuera de las instalaciones de la Institución debe seguir los procedimientos establecidos por el proceso de TICS

- La E.S.E Hospital San José de Ortega, debe identificar los riesgos potenciales que puede generar destruir, reparar o eliminar equipos y medios de almacenamiento. Para ello, debe definir e implementar los mecanismos de protección de datos personales y controles adecuados para que la información sensible contenida en ellos sea eliminada de manera segura.

6.2.1.2.4 No repudio.

- Estos servicios se utilizarán cuando sea necesario resolver disputas acerca de la ocurrencia de un evento o acción. Su objetivo es proporcionar herramientas para evitar que aquél que haya originado una transacción electrónica niegue haberla efectuado.

6.2.1.2.5 Protección y confidencialidad.

- Todos los empleados deberán conocer las restricciones al tratamiento de datos personales y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. La Hospital redactará un "Compromiso de Confidencialidad", el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por la Hospital.

6.2.1.2.6 Registro y auditoria.

- Se generarán registros de auditoría que contengan excepciones y otros eventos relativos a la seguridad. Los registros de auditoría deberán incluir la identificación del usuario, la fecha y hora de inicio y terminación, la identidad o ubicación de la terminal, un registro de intentos exitosos y fallidos de acceso al sistema y un registro de intentos exitosos y fallidos de acceso a datos y otros recursos.
- Se desarrollarán procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios sólo estén desempeñando actividades que hayan sido autorizadas explícitamente.

6.2.1.2.7 Capacitación y sensibilización.

- Todos los empleados del Organismo y, cuando sea pertinente, los usuarios externos y los terceros que desempeñen funciones en el organismo recibirán una adecuada capacitación y actualización periódica en materia de la política, normas y procedimientos de la Entidad. Esto comprende los requerimientos de seguridad y las responsabilidades legales, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

6.2.1.2.8 Gestión de incidentes.

- Los incidentes relativos a la seguridad serán comunicados a través de canales apropiados tan pronto como sea posible. Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que ante la detección de un supuesto incidente o violación de la seguridad, el Responsable de Seguridad Informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

- Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Responsable de Seguridad Informática.

6.2.2 Postulados de los Procedimientos de Seguridad de la Información

Los procedimientos de Seguridad de la Información que adoptará la Entidad durante la siguiente fase con el fin definir como serán implementadas las políticas, mejores prácticas y guías basados en los controles de S.I., según la norma ISO/IEC 27001, se regirán bajo los siguientes principios:

6.2.2.1 Seguridad del recurso humano.

6.2.2.1.1 Capacitación y sensibilización del personal.

Se redactará guía que describa sistemáticamente como identificar, facilitar y efectuar las actividades de sensibilización, entrenamiento y/o educación según el rol y necesidad dentro del proceso, especificando cada cuanto debe iniciar el ciclo.

6.2.2.1.2 Ingreso y desvinculación del personal.

Se postulan los procedimientos necesarios para motivar y vincular al talento humano competente que requiera el Hospital con el fin de garantizar el cumplimiento de los objetivos y funciones trazados. Igualmente, que requisitos y fases deben agotarse para su desvinculación, según el régimen de contratación del empleado.

6.2.2.2 Gestión de activos.

6.2.2.2.1 Identificación y clasificación de activos.

Se definirá la metodología para la ejecución del inventario, clasificación y etiquetado de activos de información, con el fin de conocer el nivel de importancia respecto al atributo de confidencialidad o criticidad, indicando como se realizan los traspasos entre funcionarios, su devolución definitiva y disposición final del activo.

6.2.2.3 Control de acceso.

6.2.2.3.1 Ingreso seguro a los sistemas de información.

Se redactará de forma sistémica como el Hospital debe administrar el acceso de los sistemas de información con el fin de evitar que sus contraseñas sean conocidas mediante ataques de fuerza bruta, utilizando canales cifrados para la transmisión de la información que según su clasificación se requiera, asimismo, cómo y quién puede realizar el acceso remoto a los dispositivos de la red y estipulando que aplicaciones que por su criticidad necesitan una autenticación de dos pasos.

6.2.2.3.2 Gestión de usuarios y contraseñas.

Se indicará como tiene que realizarse la creación de usuarios y su ingreso al sistema requerido, indicando la periodicidad de los cambios de las contraseñas, longitud, complejidad, decisión tomada por intentos errados de autenticación y la forma en que se debe ejecutar la trazabilidad de estas.

6.2.2.4 Criptografía.

No se estima necesaria su implementación a mediano plazo, debido a la complejidad que puede representar su implementación y según el riesgo analizado de los activos actuales. Se seguirá utilizando el cifrado tradicional de los sistemas implementados actualmente.

6.2.2.5 Seguridad física y del entorno.

6.2.2.5.1 Control de acceso físico.

Se deberá detallar como se efectúa el ingreso autorizado a las diferentes áreas del hospital del personal, según una clasificación preestablecida e indicando el responsable y la forma en que se deban otorgar autorizaciones temporales a personal no autorizado. Asimismo, deberá definir como se realiza y quien es el responsable del seguimiento a los controles de accesos establecidos.

6.2.2.5.2 Protección de activos.

Se indicará metodológicamente las medidas efectuadas con el fin de salvaguardar los dispositivos e instalaciones, según su grado de confidencialidad y el riesgo al que podrían estar expuestos por amenazas naturales o causadas por el hombre y como los dispositivos informáticos institucionales podrán ser retirados del Hospital. Igualmente, especificará como, quien y cuando ejecutará el mantenimiento preventivo y correctivo de los equipos informáticos.

6.2.2.6 Seguridad de las operaciones.

6.2.2.6.1 Gestión de cambios.

Se especifica cómo se realiza el control de cambios en los procesos, las instalaciones y los sistemas teniendo en cuenta las pruebas previas, la planificación, la identificación, registro, entre otros aspectos de las modificaciones efectuadas, donde se consideren valor del impacto, la indisponibilidad del servicio, comunicaciones y ejecuciones de "rollback"

6.2.2.6.2 Gestión de capacidad.

Se deberá indicar como el Hospital gestiona la capacidad de los sistemas de información críticos, para que siempre se encuentren disponibles con el menor costo posible, para que se cumplan los niveles de servicio planteados, minimizando el riego de interrupción en la prestación de los servicios.

6.2.2.6.3 Separación de ambientes.

Se Indicará como La Entidad realiza las pruebas para determinar cómo es el comportamiento de las aplicaciones nuevas o modificadas, como se hacen los ajustes, su compatibilidad con

las otras aplicaciones y el sistema en general antes de insertarlas en el ambiente de producción.

6.2.2.6.4 Protección contra códigos maliciosos.

Se definirá sistemáticamente la forma en que el Hospital protegerá sus activos de información de infección con software malicioso, indicando el uso de software o hardware especifico según el nivel de criticidad otorgado al activo, para evitar el impacto en su disponibilidad, integridad y/o confidencialidad.

6.2.2.7 Seguridad de las comunicaciones.

6.2.2.7.1 Aseguramiento de servicios en la red.

Se especifica la metodología adoptada por el Hospital para fortalecer la disponibilidad de las diferentes redes de datos de la Entidad, señalando los controles de seguridad adoptados en cada uno de los medios guiados o no guiados que protejan la confidencialidad e integridad de los datos y la forma en que se audita para verificar acciones sospechosas sobre los mismos.

6.2.2.7.2 Transferencia de información.

Se indica cual es el procedimiento para transmisión de la información según el área a comunicar o actor externo, protegiéndola de ser interceptada, copiada, modifica o destruida, para lo cual tendrá en cuenta los acuerdos de confidencialidad y no divulgación, respecto a su actualización, duración, acciones en caso de incumplimiento, entre otros.

6.2.2.8 Relaciones con los proveedores.

6.2.2.8.1 Tratamiento de la seguridad en los acuerdos con los proveedores.

Se deberá indicar como el Hospital establece, acuerda, aprueba y divulga los requerimientos y obligaciones relacionados con la seguridad de la información, respecto a las personas o establecimientos comerciales que le brindan servicios y/o productos, y las condiciones legales, , reglas de uso aceptable de la información, manejo de gestión de incidentes, descripción de la información que se divulga, resolución de conflictos, informes parte del proveedor, auditorías al servicio y gestión de cambios.

6.2.2.9 Adquisición, desarrollo y mantenimiento de sistemas de información.

6.2.2.9.1 Adquisición, desarrollo y mantenimiento de software.

Se describirá como el Hospital realiza las pruebas necesarias a las aplicaciones propias o adquiridas a terceros, previendo que cumplen con los requerimientos de seguridad apropiados y señalando los tipos de documentos para la realización de pruebas.

6.2.2.9.2 Control software.

Se estipula como el Hospital debe efectuar el inventario del software en la entidad, determinando quien, y como se debe efectuar la instalación de las aplicaciones y auditar que esto se cumpla, igualmente que las licencias de software obtenido de terceros cumplan con las normas legales.

6.2.2.10 Gestión de incidentes de seguridad de la información.

Se especifica metodológicamente como se deben reportar los incidentes que ocurren en el hospital por parte de los usuarios o propietarios de la información y a quien se deben reportar, con las medidas que se toman para identificar, detener, recoger evidencias para evitar que el

incidente se repita. Igualmente, indicará en que momento deberá activarse el Plan de Continuidad del Negocio.

6.2.2.11 Aspectos de seguridad de la información de la gestión de continuidad de negocio.

Se debe especificar el procedimiento a seguir en caso de desastre, teniendo en cuenta cómo y cuándo se restablecerán sus servicios teniendo en cuenta la prioridad y las etapas a ejecutar, donde se incluya la forma de comunicación con entidades externas para lograr este fin.

6.2.3 Roles y Responsabilidades

6.2.3.1 Área de seguridad informática.

Esta sección es la encargada de brindar la protección a la infraestructura tecnológica del Hospital y responsable del tratamiento de datos que contienen los diferentes dispositivos y los que circulan por la red, cumpliendo las siguientes funciones:

- Establecer y documentar las responsabilidades de la organización en cuanto a seguridad de información.
- Mantener la política y estándares de seguridad de información de la organización.

- Identificar objetivos de seguridad y estándares del Hospital (prevención de virus, uso de herramientas de monitoreo, etc.)
- Definir metodologías y procesos relacionados a la seguridad de información.
- Comunicar aspectos básicos de seguridad de información a los empleados del Hospital. Esto incluye un programa de concientización para comunicar aspectos básicos de seguridad de información y de las políticas del Hospital.
- Desarrollar controles para las tecnologías que utiliza la organización. Esto incluye el monitoreo de vulnerabilidades documentadas por los proveedores.
- Monitorear el cumplimiento de la política de seguridad del Hospital
- Controlar e investigar incidentes de seguridad o violaciones de seguridad.
- Realizar una evaluación periódica de vulnerabilidades de los sistemas que conforman la red de datos del Hospital.

6.2.3.2 Custodio de información.

- Administrar accesos a nivel de red (sistema operativo).
- Administrar accesos a nivel de bases de datos.
- Administrar los accesos a archivos físicos de información almacenada en medios magnéticos (diskettes, cintas), ópticos (cd) o impresa.

- Implementar controles definidos para los sistemas de información, incluyendo investigación e implementación de actualizaciones de seguridad de los sistemas (service packs, fixes, etc.) en coordinación con el área de seguridad informática.
- Desarrollar procedimientos de autorización y autenticación.
- Monitorear el cumplimiento de la política y procedimientos de seguridad en los activos de información que custodia.
- Investigar brechas e incidentes de seguridad.
- Entrenar a los empleados en aspectos de seguridad de información en nuevas tecnologías o sistemas implantados bajo su custodia.
- Asistir y administrar los procedimientos de backup, recuperación y plan de continuidad de sistemas.

6.2.3.3 Usuario.

- Mantener la confidencialidad de las contraseñas de aplicaciones y sistemas.
- Reportar supuestas violaciones de la seguridad de información.
- Asegurarse de ingresar información adecuada a los sistemas.
- Adecuarse a las políticas de seguridad del Hospital.
- Utilizar la información del Hospital únicamente para los propósitos autorizados.

6.2.3.4 Propietario de información.

- Asignar los niveles iniciales de clasificación de información.
- Revisión periódica de la clasificación de la información con el propósito de verificar que cumpla con los requerimientos del negocio.
- Hay que asegurar que los controles de seguridad aplicados sean consistentes con la clasificación realizada.
- Determinar los criterios y niveles de acceso a la información.
- Revisar periódicamente los niveles de acceso a los sistemas a su cargo.
- Determinar los requerimientos de copias de respaldo para la información que les pertenece.
- Tomar las acciones adecuadas en caso de violaciones de seguridad.
- Verificar periódicamente la integridad y coherencia de la información producto de los procesos de su área.

6.2.3.5 Control interno

- El personal de auditoria interna es responsable de monitorear el cumplimiento de los estándares y guías definidas en las políticas internas. Una estrecha relación del área de auditoria interna con el área de seguridad informática es crítica para la protección de los activos de información. Por lo tanto, dentro del plan anual de evaluación del área

de auditoria interna se debe incluir la evaluación periódica de los controles de seguridad de información definidos por el Hospital. Auditoria interna debe colaborar con el área de seguridad informática en la identificación de amenazas y vulnerabilidades referentes a la seguridad de información del Hospital.

6.2.4 Metodología Realización De Inventario De Activos De Información

El procedimiento que se propuso para la gestión de los activos en el Hospital de San José de Ortega se basa en los lineamientos de Gobierno en Línea, observado en la figura 31:

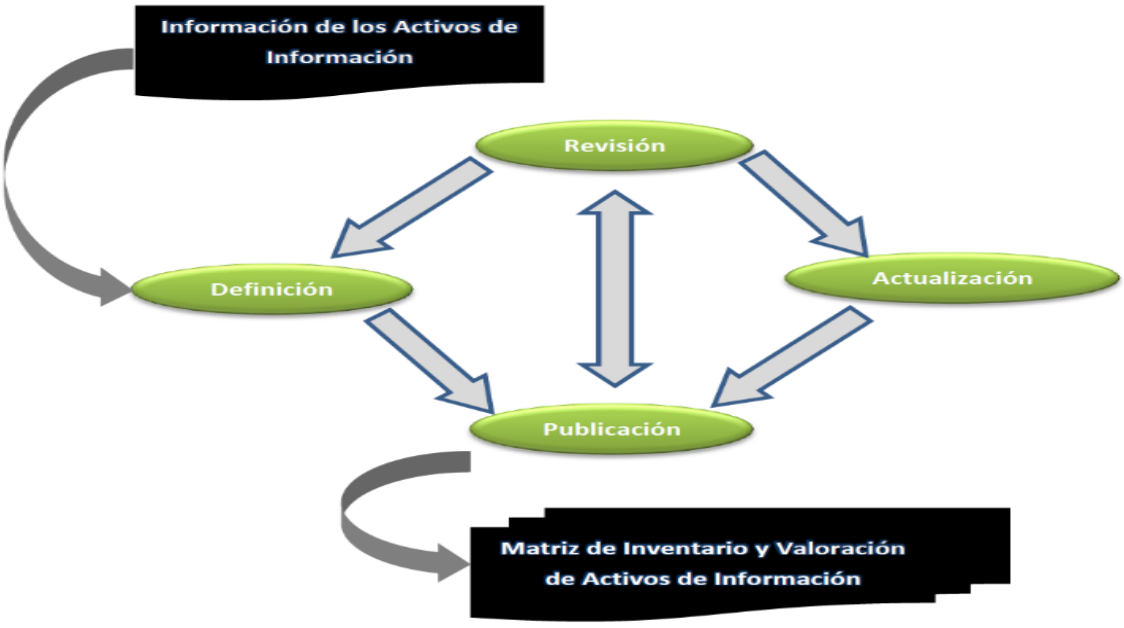


Figura 31. Procedimiento Inventario de Activos

- La definición consiste en determinar qué activos de información van a hacer parte del inventario.
- La revisión se refiere a la verificación que se lleva a cabo para determinar si un activo de información continúa o no siendo parte del inventario, o si los valores de evaluación asignados en el inventario y clasificación de activos de Información deben ser modificados.
- Una vez se ha definido qué cambios se realizarían en el inventario, desde cada proceso, se procede a actualizar el inventario de activos de información.
- La Publicación es dar a conocer al propietario del activo su situación actual.

La ejecución del inventario de activos debe ser acorde a lo estipulado en el dominio 8 Gestión de Activos del anexo A de la norma ISO 27001:2013, ISO 27002, e ISO 27005 en los siguientes aspectos:

- Inventario de activos: todos los activos deben estar claramente identificados y la entidad debe elaborar y mantener un inventario de estos.
- Propiedad de los activos: los activos de información del inventario deben tener un propietario.

- Clasificación de la información: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

- Etiquetado y manipulado de la información: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.

Para su clasificación se utilizan sus pilares fundamentales, La Confidencialidad, Integridad y Disponibilidad a los cuales se les designa un nivel, alto, medio y bajo según su criticidad:

Niveles de Evaluación de Activo	
ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Tabla 16. Niveles de Evaluación de Activo

Una vez establecido el nivel y con base en el principio de la Confidencialidad se procede a su clasificación:

Criterios de Clasificación de Activo		
Confidencialidad	***Integridad***	***Disponibilidad***
Información Publica Reservada	Alta (A)	Alta (1)

Información Publica Clasificada	Media (M)	Media (2)
Información Pública No Clasificada	Baja (B) No Clasificada	Baja (3) No Clasificada

Tabla 17. Criterios de Clasificación de Activo

Se deben realizar revisiones cada seis meses, o con ocurrencia de alguno de estos eventos:

- Actualizaciones al proceso al que pertenece el activo.
- Adición de actividades al proceso.
- Inclusión de nuevos registros de calidad, nuevos registros de referencia o procesos y procedimientos.
- Inclusión de un nuevo activo.
- Desaparición de un área, proceso o cargo en la entidad que tenía asignado el rol de propietario o custodio (Cambios Organizacionales).
- Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.
- Cambios físicos de la ubicación de activos de información.

El Inventario de activos de información es un documento clasificado y no puedes sufrir modificaciones por usuarios no autorizados. El acceso está permitido solamente al propietario del proceso con autorización del Jefe de Sistemas.

Los activos que aún no se hayan clasificado se tomarán como “No Clasificados” y se tratarán con el nivel más alto de evaluación.

Para el etiquetado de los Activos se siguen los siguientes parámetros:

Se etiquetarán todos los Activos de Información que estén clasificados según el esquema clasificación en Confidencialidad, Integridad y disponibilidad.

Se etiquetará el nivel de clasificación con relación a Confidencialidad, Integridad y Disponibilidad.

Si un Activo de Información en formato impreso no se encuentra etiquetado debe ser tratado en todos sus niveles (Confidencialidad, Integridad y Disponibilidad) como NO CLASIFICADA.

Cada Activo de Información debe ser etiquetado teniendo en cuenta el esquema de clasificación, y en el campo correspondiente diligenciar la clasificación de la siguiente forma: {Clasif.Confidencialidad} - {Clasif.Integridad} - {Clasif.Disponibilidad}.

Para los activos clasificados en confidencialidad como INFORMACION PUBLICA RESERVADA se podría utilizar la etiqueta IPR, INFORMACION PUBLICA CLASIFICADA IPC y INFORMACION PUBLICA, IPB. Para los activos clasificados en

integridad como ALTA se utilizará la etiqueta A, MEDIA, M y BAJA, B. Para los activos clasificados en disponibilidad como ALTA se utilizará la etiqueta 1, MEDIA, 2 y BAJA, 3.

Este procedimiento se realiza por las áreas de informática, gestión de calidad y archivo del Hospital.

6.2.5 Valoración y Tratamiento del Riesgo

Una vez identificados los activos y la existencia de sus controles, amenazas y vulnerabilidades realizados en la etapa de diagnóstico, se efectúa la evaluación del riesgo basados en la guía del Departamento de Administrativo de la Función Pública, DAFP, en la cual esta evaluación se realiza de forma cualitativa estableciendo una matriz de Calificación, Evaluación y respuesta a los Riesgos presenta la forma de calificar los riesgos con los niveles de impacto y probabilidad establecidos anteriormente, así como las zonas de riesgo presentando la posibles formas para su tratamiento.

Para esto se debe tener en cuenta dos términos importantes, como es el de la probabilidad, relacionado con la posibilidad de que ocurra el riesgo, el cual se mide bajo criterios de ocurrencia, cuantas veces ha ocurrido en un periodo de seis meses, o bien, examinando factores internos o externos presentes que puedan causar el riesgo. La otra definición es la del impacto que es el efecto causado por que el riesgo fue materializado.

Ahora bien, teniendo en cuenta estos dos conceptos, probabilidad e impacto, se realiza una matriz que permita asociar el riesgo asociado a un activo específico dentro de una zona

y que soporte el tratamiento apropiado que debe adoptarse en cada caso en particular. El tratamiento del riesgo de la seguridad del activo de información se debe enmarcar en alguna de las siguientes cuatro opciones:

- Aceptarlo cuando la implementación de control de seguridad es más costosa que el impacto causado al activo y la zona de riesgo es baja o moderada
- Disminuirlo con la aplicación de un control de seguridad.
- Transferirlo o Compartirlo para minimizar los costos del impacto asociado.
- Evitarlo deteniendo la ejecución de la actividad que lo coloca en riesgo o hacerla de una forma diferente.

La matriz para la evaluación de las Zonas de riesgos es la siguiente:

Tabla 18. Matriz para la evaluación de las Zonas de riesgos. Adaptado DAFP

Probabilidad	***Impacto***				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

- Para la zona Baja(B) se acepta el riesgo.
- Para la zona Media(M) se asume o se reduce.
- Para la zona Alta(A) se reduce, se evita o se trasfiere.
- Para la zona Extrema(E) se reduce, se evita o se trasfiere.

Con base en esta matriz se realizar el análisis de riesgo, el cual se ejemplifica según información obtenida durante la fase de diagnóstico relacionada con el control de acceso:

Tabla 19. Ejemplo Análisis de Riesgo

Análisis de Riesgos *Clasificación: Control de Acceso*					
Objetivo: Establecer medios idóneos que permitan el acceso exclusivo a las personas autorizadas según su nivel de seguridad a sitios y sistemas de información.					
Riesgo	*Calificación*		*Tipo de Impacto*	*Zona de Riesgo*	*Respuesta*
	Probabilidad	Impacto			
Fuga de Información	3	4	Confidencialidad	Extrema	Reducir, evitar o transferir

6.2.6 Resultado Etapa de Planeación

Ejecutada las fases de diagnóstico y de planeación se puede concluir que se deben seguir realizando ciertas actividades para ir cerrando la brecha existente y permitir que el Hospital el objetivo planteado que es la implantación del Modelo de Seguridad de la Información y salvaguardar los datos personales de sus usuarios y de sus transacciones institucionales, para lo cual se deben efectuar las siguientes acciones en un término no superior a 18 meses, como se muestra en la figura 32:

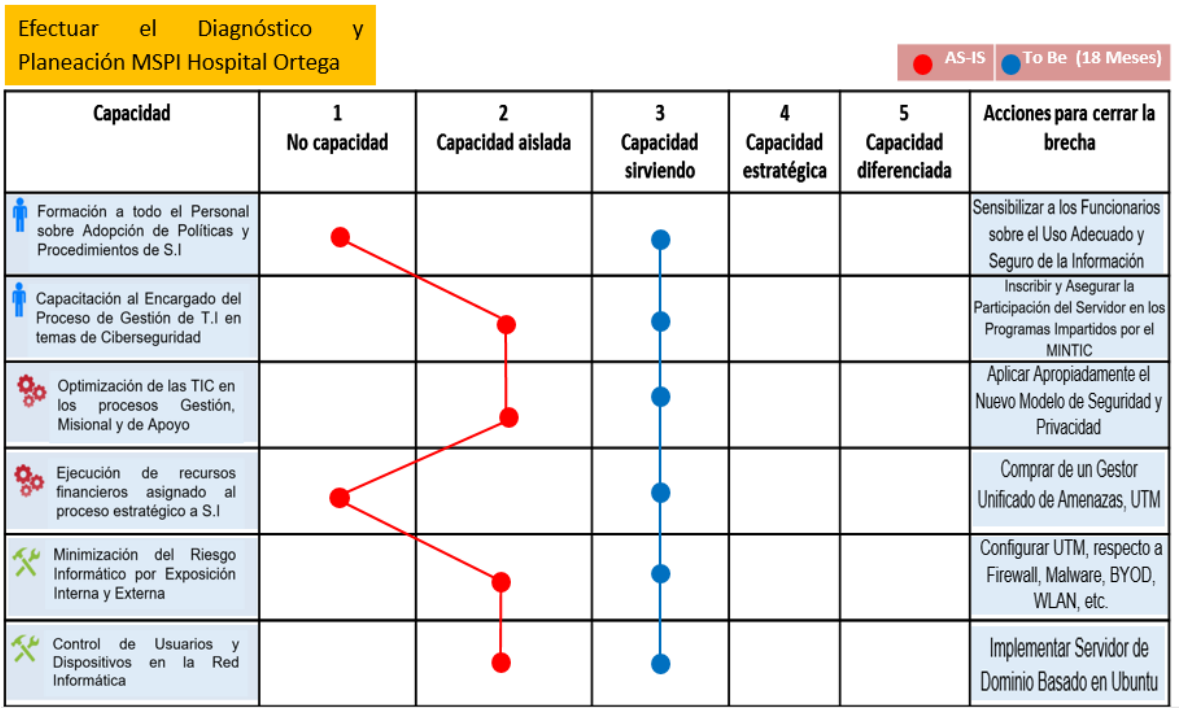


Figura 32. Acciones para Cerrar la Brecha

7. Comunicación de Resultados

Se realiza socialización al gerente del hospital, doctor Yamil Rodríguez Garza; a la doctora Julie Alexandra Joya Monroy, asesora de calidad; al ingeniero Uriel Alfonso Ortiz Montaña, gestor de la oficina de tecnología de la información y a la doctora Elida Méndez Riaño, secretaria de servicio social de la alcaldía del municipio de Ortega e integrante de la junta directiva de la Institución.

Reunión en la cual se informa sobre los resultados obtenidos durante el desarrollo del proyecto y se resuelven las dudas planteadas durante el desarrollo de esta actividad.

Igualmente se dan a conocer las recomendaciones, conclusiones y la necesidad que existe de dar continuidad al Modelo de Seguridad y Privacidad, y el trabajo futuro realizar.

Es de anotar que durante el desarrollo de la presentación hubo especial interés por parte de los presentes en los aspectos relacionados con el ingreso remoto realizado al servidor donde se encuentra su principal sistema de información, donde se explicó la forma de ejecución de la prueba y donde por petición del gerente se mencionaron ciertas pautas para mitigar las vulnerabilidades halladas.

Otro punto tratado de interés y crucial para un desarrollo armónico de su gestión de infraestructura tecnológica y por ende de la seguridad y privacidad de la información es la inexistencia del Plan Estratégico de Tecnológico de la Información, PETI, lo cual es de vital importancia y debe ser el primer paso a observar para el desarrollo de futuros trabajos de este tipo para una ejecución estratégica planificada, solicitando el gerente de esta E.S.E apoyo para el estudio y redacción del mismo teniendo en cuenta la visión obtenida durante el desarrollo de este proyecto.

Se anexan imágenes tomadas durante la sesión efectuada y la cuales se pueden observar en las figuras 33 y 34, y donde se observan los intervinientes comenzado por el expositor y ejecutor del proyecto, siguiendo por su lado izquierdo con el gestor informático, el gerente,

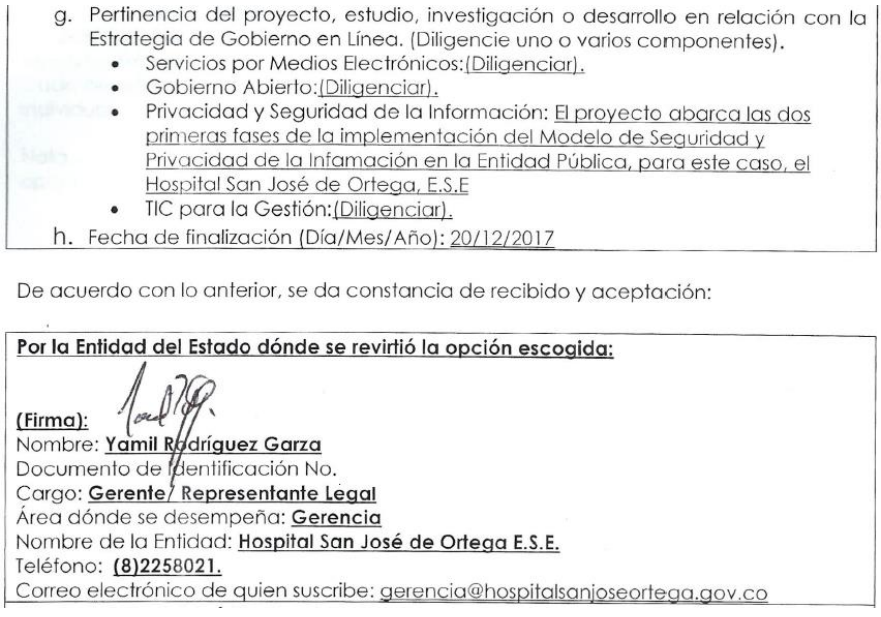
la integrante de la junta directiva y por último la asesora de calidad de esta empresa social del estado.

Figura 33. Fotografía Sensibilización MSPI Alta Gerencia

Se observa desde otro ángulo el desarrollo la sensibilización del Modelo:

Figura 34. Fotografía Sensibilización MSPI Alta Gerencia

Asimismo, la alta gerencia del Hospital recibe y acepta el trabajo realizado en esta entidad del estado como queda constancia en la figura 35*:*



g. Pertinencia del proyecto, estudio, investigación o desarrollo en relación con la Estrategia de Gobierno en Línea. (Diligencie uno o varios componentes).
- Servicios por Medios Electrónicos:(Diligenciar).
- Gobierno Abierto:(Diligenciar).
- Privacidad y Seguridad de la Información: El proyecto abarca las dos primeras fases de la implementación del Modelo de Seguridad y Privacidad de la Infamación en la Entidad Pública, para este caso, el Hospital San José de Ortega, E.S.E
- TIC para la Gestión:(Diligenciar).

h. Fecha de finalización (Día/Mes/Año): 20/12/2017

De acuerdo con lo anterior, se da constancia de recibido y aceptación:

Por la Entidad del Estado dónde se revirtió la opción escogida:

(Firma):
Nombre: **Yamil Rodríguez Garza**
Documento de Identificación No.
Cargo: **Gerente/ Representante Legal**
Área dónde se desempeña: **Gerencia**
Nombre de la Entidad: **Hospital San José de Ortega E.S.E.**
Teléfono: **(8)2258021.**
Correo electrónico de quien suscribe: gerencia@hospitalsanjoseortega.gov.co

Figura 35. Imagen Aceptación Trabajo Alta Gerencia

8. Conclusiones

Con la ejecución del Diagnóstico y Planeación del MSPI en el Hospital San José de Ortega, se formaliza un paso importante para dar cumplimiento a la ley 1341 de 2009, el cual debe ser culminado para el año 2020.

La cultura organizacional a nivel de seguridad de la información se incrementó en un 30%, debido a las actividades desarrolladas por el trabajo realizado, lo cual permite ir cerrando la brecha para que el Hospital logre alcanzar las metas programadas por la estrategia de gobierno en línea, por cuanto se han ejecutado el diagnóstico y la fase de planeación dentro de la metodología planteada por el Ministerio de las Tecnología y Comunicación de Colombia en su estrategia de Gobierno En Línea, GEL.

Además, se avanza para conseguir que los datos personales sensibles especialmente de los pacientes del Hospital se aseguren, con el fin de evitar que sea conocida o modificada por personas no autorizadas, o bien, no esté disponible cuando se requiera.

Por otra parte, desde el punto de vista del candidato a magister ejecutor, con la realización del presente proyecto se afianzan los conocimientos obtenidos durante la maestría especialmente en los ámbitos de gestión de seguridad en tecnologías de la información, y de gobierno y gestión de servicios en tecnologías de información, enriqueciendo sus

conocimientos y experiencia como profesional en las áreas relacionadas con la gestión de las TIC.

Específicamente se llega a las siguientes conclusiones:

- ✓ Se logra determinar el estado actual de la gestión de seguridad y privacidad de la información en el Hospital de Ortega, con el uso de pruebas técnicas, entrevistas, encuestas y observación directa.
- ✓ Se conoce lo que comprenden por seguridad y privacidad de la información los trabajadores de la Entidad, según los resultados de las entrevistas informales y encuestas efectuadas a funcionarios de las diferentes dependencias en los procesos de gestión, misional y de apoyo.
- ✓ Se Identifican las amenazas y vulnerabilidades respecto a la seguridad de la información que posee el Hospital San José de Ortega, en los aspectos de hardware, red, acceso de datos y sistema de información a través de pruebas técnicas, entrevistas y observación directa.
- ✓ Se define la política y procedimientos de seguridad de la información en la entidad objetivo, acorde con las necesidades y expectativas percibidas por los grupos de interés que permiten valorar los controles aplicables a sus procesos misionales y de apoyo acordes a los principios y objetivos institucionales.

- ✓ Se propone la metodología para la realización de inventario de activos y gestión del riesgo, basado en el método utilizado por el Departamento de Administrativo de la Función Pública, DAFP, por ser el procedimiento general adoptado por las instituciones gubernamentales en el ámbito nacional, mencionando sus principales conceptos.

- ✓ Se logra concienciar al área de sistemas del Hospital que existen ciertas vulnerabilidades explotables en un servidor de datos principal, que pondrían en riesgo la confidencialidad, disponibilidad e integridad de los datos de los Pacientes, con la realización de unas pruebas de vulnerabilidad que evidenciar unas debilidades en el sistema.

- ✓ El respaldo de la Gerencia y de los Jefes de Oficina de las diferentes dependencias en cualquier proyecto de implantación de un MSPI es fundamental para llevar a buen término cada uno de los subprocesos del Modelo.

- ✓ La limitación que tienen estas entidades municipales en su presupuesto no les permite implementar en forma completa el modelo planteado por el MINTIC, por tanto, se debe analizar los temas más críticos, teniendo en cuenta que las amenazas que se ciernen sobre éstas no revisten un grado de riesgo alto.

- ✓ El principal reto que debe afrontar el Hospital San José de Ortega es el de inculcar a todo el personal sobre la cultura de la seguridad de la información para evitar la pérdida de datos sensibles que retrasen la consecución de los objetivos trazados en

cada proceso, causado no intencionalmente, sino inconscientemente por negligencia o falta de experiencia.

9. Recomendaciones

Teniendo en cuenta que el eslabón más débil en la cadena de la seguridad son las personas, es necesario que efectúen sensibilizaciones grupales a los funcionarios del Hospital de forma periódica según su rol y responsabilidad, teniendo en consideración temas como: políticas y procedimientos de seguridad de información adoptados por el Hospital, instalación de software no autorizado, uso adecuado del correo electrónico y dispositivos extraíbles. Asimismo, es conveniente que el jefe de la Oficina de Sistemas esté permanentemente actualizado en temas de nuevas amenazas que puedan impactar los activos de la Entidad e instalar o actualizar los controles necesarios que permitan reducir el riesgo.

En cuanto a la infraestructura tecnológica del Hospital se hace necesario que la gerencia obtenga los recursos necesarios para realizar prioritariamente estas tareas:

- ✓ Instalar un servidor de dominio que le permita gestionar, entre otros aspectos, los privilegios de usuarios y equipos.
- ✓ Actualizar los sistemas operativos a la última versión y los equipos que no se pueda realizar esta labor, debido a la imposibilidad de migrar una aplicación, mantenerlo permanentemente parchado, monitoreado y aislado de la red corporativa.

- ✓ Instalar cableado estructurado para la red corporativa con el fin de evitar el uso de redes inalámbricas, que pueden ser accedidas sin control y son muy susceptibles a ataques de denegación de servicio en un rango geográfico amplio.
- ✓ Realizar "hardening" al servidor Linux que contiene el sistema SIHOS, por cuanto en las pruebas realizadas fue vulnerado con herramientas de uso gratuito de fácil acceso al público en general.
- ✓ Comprar, instalar y configurar un Gestor Unificado de Amenazas, que tenga integrado Firewall, antimalware, antispam, IDS, BYOD, con sus respectivas licencias periódicas.

10. Trabajo a Futuro

Concluir el Modelo de Seguridad y Privacidad de la Información, para lo cual se debe implementar lo planificado en el presente trabajo e ir evaluando lo planeado durante la ejecución para lograr una mejora continua dentro de cada uno de los procesos, con el fin de lograr una mayor eficiencia dentro del modelo planteado según las necesidades y requerimientos específicos del Hospital, con base en los recursos económicos y humanos que posee actualmente.

Durante la fase de implementación, las tareas prioritarias para efectuar son la capacitación a los funcionarios sobre el uso seguro de los sistemas de información a través de cursos

virtuales obligatorios con el apoyo del Ministerio de la Tecnología y las Comunicaciones, por cuanto el presupuesto para temas de seguridad es escaso en esta Entidad.

Asimismo, el servidor Linux que contiene la base de datos hospitalaria, SIHOS, se le realizará una nueva auditoría en el tema para comprobar si ya sean corregidos errores de configuración de la seguridad, como deshabilitar servicios innecesarios, desinstalar aplicaciones en desuso, ausencia de firewall, registros de eventos funcionando, utilización de SSH 2, permitir usuarios específicos entre otros aspectos.

Otro punto neurálgico para ejecutar es la instalación de la red cableada completa, pero es difícil su implementación debido a los altos costos que esto acarrea, agravado por la expectativa de un cambio de sede. Por lo cual de forma transitoria se rediseñará la disposición de los equipos informáticos, segmentando la red con el uso de VLAN según grupos de trabajo y se configurará la conexión inalámbrica tomando más medidas de seguridad, como filtrado MAC y ocultando el SSID, con el fin el de hacerle más difícil la tarea a un posible atacante.

Referencias Bibliográficas

Aguirre Cardona, J (2013). Diseño Del Sistema De Gestión De Seguridad De La Información Para El Grupo Empresarial La Ofrenda. Recuperado de: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/4117/0058A284.pdf;jsessionid=01C E29BB3AEA80D6ADBA64979514EDC5?sequence=1

Álvarez Basaldúa, L. (2005). Seguridad En Informática (Auditoria de Sistemas). Recuperado de: http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf

Alcaldía de Bogotá, (2009). Ley 1341 de 2009 Nivel Nacional. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=36913

Alcaldía de Bogotá, (2014). Decreto 2573 de 2014 Nivel Nacional. Recuperado de: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=60596

Alcaldía de Bogotá, (2015). Decreto Único Reglamentario 1078 de 2015 Nivel Nacional. http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=62513

Barrantes Porras, G (2012). Diseño e Implementación De Un Sistema de Gestión De Seguridad de Información En Procesos Tecnológicos. Recuperado de:

http://www.repositorioacademico.usmp.edu.pe/bitstream/usmp/609/3/barrantes_ce.pdf

Bermúdez, E., Malaver, N., Niño, E., Quintero, J., Santamaría, C…& Rivera, H. (2011). Hospital del Rosario. Documentos de Investigación. Recuperado de: http://www.urosario.edu.co/urosario_files/75/75b1a202-d1e1-4cc2-a66e-10692914a1c2.pdf

Bernal López, W. (2015). Diagnosticar y asesorar la implantación de un sistema SGSI que permita controlar y gestionar todos los procesos relacionados con la información. Recuperado de http://hdl.handle.net/10596/3509

Calderón Sánchez, A. (2015). Implementación del SGSI en el área de redes de COMPUSERVER basado en la norma ISO/IEC 27001:2013. Recuperado de http://hdl.handle.net/10596/3676

Cao, J. Sistemas de Gestión Seguridad de la Información. Los malos 3, Los buenos 0. Recuperado de: http://sgsi-iso27001.blogspot.com.co/2014/06/ciberseguridad-minuto-yresultado-los.html

CISSP, (2018). Security Models and Architecture, chapter 5. Recuperado de: http://media.techtarget.com/searchSecurity/downloads/29667C05.pdf

Consejo Técnico de la Contaduría Pública, (2017). Direccionamiento Estratégico. Recuperado de: https://www.slideshare.net/emirtorres/01-direccionamiento-estrategico

Corletti, A. (2006). Análisis de ISO-27001:2005. [En línea], (abril 2006). [Consultado 06 de mayo de 2015]. Disponible en Internet: www.criptored.upm.es/guiateoria/gt_m292g.htm

Doria Corcho, A. (2015). Diseño de un sistema de gestión de la seguridad de la información mediante la aplicación de la norma internacional ISO/IEC 27001:2013 en la oficina de sistemas y telecomunicaciones de la Hospital de Córdoba. Recuperado de http://hdl.handle.net/10596/3624

Empresa Tecnologías Sinergia S.A.S. (2017). SIHOS WEB cumple con las exigencias actuales del sector de la salud en Colombia. Recuperado de: http://sinergiaonline.com/sihos-web/

Hospital San José de Ortega, (2017). Página Principal sitio web Entidad. Recuperado de: http://hospitalsanjoseortega.gov.co/

Hospital San José de Ortega, (2017). Portafolio de Servicios 2017.

INCIBE, (2017). Gestión de Riesgos, Una Guía de Aproximación para el Empresario. Recuperado de: https://www.incibe.es/extfrontinteco/img/File/empresas/guias/Guia_gestion_riesgos/guiagestionriesgos.pdf

ISOTOOLS, (2017). ¿Qué es un Sistema de Gestión de Seguridad de la Información basado en la norma ISO 27001? Recuperado de: https://www.isotools.org/2016/07/07/sistema-gestion-seguridad-la-informacion-basado-la-norma-iso-27001/

Gutiérrez, C (2015). Lo que no debes pasar por alto para gestionar la seguridad de la información. Recuperado de: http://revista.seguridad.unam.mx/numero22/lo-que-no-debes-pasar-por-alto-para-gestionar-la-seguridad-de-la-informacion

Guzmán García, A. (2015). Diseño de un sistema de gestión de la seguridad informática –SGSI–, para empresas del área textil en las ciudades de Itagüí, Medellín y Bogotá D.C., a través de la auditoría. Recuperado de http://hdl.handle.net/10596/3448

Guzmán Silva, C (2015). Diseño De Un Sistema De Gestión De Seguridad De La Información Para Una Entidad Financiera De Segundo Piso. Recuperado de:

http://repository.poligran.edu.co/bitstream/10823/746/1/Proyecto%20de%20Grado%20SGSI%20-%20IGM-%20CarlosGuzman%20(FINAL).pdf

ISO2700, (2018). El portal de ISO 27001 en español. Recuperado de: http://www.iso27000.es/iso27000.html

Jojoa Paz, D. (2016). Diseño de un sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO 27001: 2013 para la red inalámbrica de la empresa innovación global S.A, ubicada en el municipio de Sibundoy Putumayo. Recuperado de http://hdl.handle.net/10596/6146

Quintero Madroñero, J. (2015). Creación e implantación del sistema de gestión de seguridad de la información (SGSI) bajo el estándar ISO/IEC 27001:2013 para la institución educativa Luis Carlos Galán de Villa Garzón Putumayo. Recuperado de http://hdl.handle.net/10596/3625

Ministerio de Tecnologías de la Información y las Comunicaciones. (2017). Manual Estrategia de Gobierno en Línea. Recuperado de: http://estrategia.gobiernoenlinea.gov.co/623/articles-7941_manualGEL.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Modelo de Seguridad y Privacidad de la Información. Recuperado de: http://estrategia.gobiernoenlinea.gov.co/623/articles-8258_recurso_1.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía Metodológica de Pruebas de Efectividad. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía Política General MSPI v1. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía Procedimiento de Seguridad de la Información. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía Roles y responsabilidades. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G4_Roles_responsabilidades.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Modelo de Seguridad y Privacidad de la Información. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía Gestión Documental. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G6_Gestion_Documental.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía Gestión de Riesgos. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Ministerio de Tecnologías de la Información y las Comunicaciones. (2016). Guía Controles de Seguridad de la Información. Recuperado de: http://www.mintic.gov.co/gestionti/615/articles-5482_G8_Controles_Seguridad.pdf

Núñez Álvarez, Y. (2015). Diseño de un SGSI para el área de automatización del proceso de báscula, de la empresa minera Sanoha Ltda. ubicada en Nobsa –Boyacá. Recuperado de http://hdl.handle.net/10596/3649

Pallas Megas, G (2009). Metodología de Implantación de un SGSI en un grupo empresarial jerárquico. Recuperado de: https://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf

PMM-SSI, (2015). ¿Qué es SGSI? Recuperado de: https://www.pmg-ssi.com/2015/07/que-es-sgsi/

Anexos

Glosario

Accesibilidad: Acceso universal a la Web, independientemente del tipo de hardware, software, infraestructura de red, idioma, cultura, localización geográfica y capacidades de los usuarios (W3C World Wide Web Consortium). En el contexto colombiano, ha venido asumiéndose como las condiciones que se incorporan en sitios y herramientas web que favorecen el que usuarios en condiciones de deficiencia tecnológica, física o sensorial o en condiciones particulares de entornos difíciles o no apropiados, puedan hacer uso de estos recursos de la Web. (W3C,2016).

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000, 2013).

Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000, 2013).

Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000, 2013).

Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoria y obviamente para determinar el grado en el que se cumplen los criterios de auditoria. (ISO/IEC 27000, 2013).

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).

Bases de Datos Personales: Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3).

Ciberseguridad: Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6).

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos

públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h).

Datos Personales Sensibles: Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3).

Derecho a la Intimidad: Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del tratamiento. (Ley 1581 de 2012, art 3).

Evaluación del riesgo: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. (NTC-ISO /IEC 27001, 2013).

GEL - (Gobierno en línea): La Estrategia Gobierno en Línea es la política Nacional de Gobierno electrónico definida a través del Decreto 1078 de 2015 artículo 2.2.9.1.1.1, que tiene como propósito lograr que los ciudadanos cuenten con servicios en línea de alta calidad, impulsar el empoderamiento y la colaboración de los ciudadanos con el Gobierno, encontrar diferentes formas para que la gestión en las entidades públicas sea óptima gracias al uso estratégico de la tecnología, y garantizar la seguridad y la privacidad de la información.(MINTIC, 2016).

Gestión de incidentes de seguridad de la información. Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000, 2013).

Hackear: Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar. (MINTIC, 2016)

Información: se refiere a toda comunicación o representación de conocimiento, como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea digital, en papel, en pantallas de computadoras, audiovisual u otro. (MINPROTECCIONSOCIAL,2016)

Mecanismos de protección de datos personales: Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimato o cifrado.

MSPI: Modelo de Seguridad y Privacidad de la Información.

Privacidad: En el contexto de este documento, por privacidad se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsable del Tratamiento de Datos:
Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000, 2013).

Seguridad de la información: Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000, 2013).

Sistema de información: se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales. (MINPROTECCIONSOCIAL,2016)

Tecnología de la información: se refiere al hardware y software operado por la entidad o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo. (MINPROTECCIONSOCIAL,2016)

Tecnologías de la Información y las Comunicaciones – TIC: Las Tecnologías de la Información y las Comunicaciones (TIC), son el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios; que permiten la compilación, procesamiento, almacenamiento, transmisión de información como: voz, datos, texto, video e imágenes (Art. 6 Ley 1341 de 2009).

Titulares de la información: Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3).

Tratamiento de Datos Personales: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad: Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000, 2013).

Vulnerabilidad: Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000, 2013).

Partes interesadas (Stakeholder): Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

Usuario: Persona o máquina delegada por un cliente para utilizar los servicios y/o facilidades de una red de telecomunicaciones. En el contexto de los servicios de telecomunicación: un

ser humano que utiliza un servicio. En un contexto técnico: un ser humano, una entidad o un proceso. (MINTIC, 2016)

Encuesta de Seguridad

I. <u>Tema: Vulnerabilidad y Amenaza</u>

1. ¿Ha recibido en los años 2016 y/o 2017, alguna clase de sensibilización, charla, taller o sensibilización relacionada con temas de Seguridad de la Información, dirigida por el Hospital?

a) Si ☐
b) No ☐

2. Ha tenido algún inconveniente, en los años 2016 y/o 2017, relacionada con pérdida de información de propiedad del Hospital?

a) Si ☐
b) No ☐

Si contestó "Si" por favor marque la causa que origina la perdida

a) Virus ☐
b) Hurto ☐
c) Sabotaje ☐
d) Incendio ☐
e) Inundación ☐
f) Olvido Contraseña ☐
g) Falla del Sistema ☐
h) Otro* ☐

*Cual? _____

3. ¿Se realiza periódicamente respaldo de la información importante del Hospital que no está contenida en el SIHOS?

a) Si ☐
b) No ☐

4. ¿En qué medio almacena la información laboral importante de su Área?

a) Dispositivo USB ☐
b) Disco Duro ☐
c) Ambos ☐

5. ¿Utiliza equipos personales (portátil) para realizar su labor del Hospital?

a) Si ☐
b) No ☐

6. ¿Conoce el nombre y contraseña de otros usuarios del SIHOS o computadores de otras áreas?

a) Si ☐
b) No ☐
c) No utiliza ☐

7. ¿Tiene acceso a internet, sin restricciones, en el computador donde guarda la información hospitalaria?

a) Si ☐
b) No ☐

8. ¿Se ha presentado algún inconveniente, este año, que no le haya permitido ingresar a su computador laboral, por más de cuatro horas?

a) Si ☐
b) No ☐
c) No utiliza ☐

II. Tema: Conocimiento de Seguridad y Privacidad de la Información

1. ¿Sabe que son las políticas de seguridad de la información de una entidad?

a) Si ☐
b) No ☐

2. ¿Sabe cuáles son los principales procedimientos de seguridad de la información de una entidad?

c) Si ☐
d) No ☐

3. ¿Conoce cuál es rol que debe desempeñar respecto a la información que administra o usa?

a) Si ☐
b) No ☐

4. ¿Sabe la diferencia entre datos personales públicos, datos personales privados y datos personales sensibles?

a) Si ☐
b) No ☐

5. ¿Conoce quién es el responsable de realizar el respaldo de la información que usted administra?

a) Si ☐
b) No ☐

6. ¿Sabe cómo se construye una contraseña segura para el acceso a sus dispositivos informáticos?

a) Si ☐
b) No ☐

7. ¿Conoce las implicaciones de carácter penal que le acarrearían un uso inadecuado de los datos y los equipos informáticos que usted utiliza con ocasión de su labor en el Hospital?

a) Si ☐
b) No ☐

8. ¿Sabe a qué se refiere el término “Ransomware”?

a) Si ☐
b) No ☐