ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DIRECCIÓN DE POSGRADOS

TEMA: "IMPLEMENTACIÓN DE UNA RED SEGURA Y UN SISTEMA DE GESTIÓN HOSPITALARIA PARA EL HOSPITAL DE ESPECIALIDADES DE FUERZAS ARMADAS"

REALIZADO POR:

J. HUGO ALVAREZ V.

MAYO DE COM.

DIRECTOR:

ING. GIOVANNI ROLDAN CRESPO

SANGOLQUÍ-ECUADOR

2013

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por el Ing. J. Hugo Álvarez V. Bajo mi supervisión, como requerimiento para la obtención del título de Máster en Gerencia de Sistemas.

Sangolquí, 19 de Diciembre del 2013.

Ing. Giovanni Roldán Crespo.

DIRECTOR

AUTORÍA DE RESPONSABILIDAD

Yo, Jorge Hugo Álvarez Vergara, declaro que el trabajo aquí descrito es de mi autoría, que no ha sido presentado por ningún grado o calificación profesional; y que he consultado las referencias bibliográficas que se incluye en este documento.

A través de la siguiente declaración cedo mis derechos de propiedad intelectual correspondiente a este trabajo, a la Universidad de las Fuerzas Armadas ESPE, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por su normativa institucional vigente.

Ing. J. Hugo ÁLVAREZ V.

Dedicatoria

A mis queridas hijas: ***Brenda Salomé, Sahián Cristal y DenebSarahí,***que sea un ejemplo y motivación para su vida profesional y sobre todo a mi esposa Xime., mujer virtuosa.

Agradecimiento

A DIOS todo poderoso a quien me debo en integridad.

A mi ***Glorioso Ejército Ecuatoriano*** en especial al Hospital de Especialidades de FFAA., por permitirme ser parte de su personal administrativo 2012 – 2014.

ÍNDICE

INDICE DE GRÁFICOS

Í NDICE TABLAS

RESUMEN

El proyecto de grado para la MGS denominado ***"IMPLEMENTACIÓN DE UNA RED SEGURA Y UN SISTEMA DE GESTIÓN HOSPITALARIA PARA EL HOSPITAL DE ESPECIALIDADES DE FUERZAS ARMADAS"*** presenta la implementación de una Red de Datos Segura, basada en la norma ISO 17799 con el fin de que el Sistema Informático de Gestión Hospitalario a instalarse fluya a través de esta red con seguridad, confiabilidad, estabilidad.

Este proyecto presenta una solución integral al sistema de gestión médico, administrativo de esta casa de salud.

Implementar una red segura basada en la norma internacional la ISO 17799 a fin de que garantice una conectividad permanente y estable para que se instale un Sistema Informático de Gestión Hospitalaria aplicando una Gestión del Cambio institucional, permitirá tener un control adecuado de la Gestión Médica y Administrativa, logrando de esta manera acatar las disposiciones del Ministerio de Salud Pública como es la de aplicar un tarifario nacional y facturar de manera automática todos los servicios que presta el HE-1.

Palabras claves: HOSPITAL MILITAR, SEGURIDAD DE REDES, IMPLEMENTACIÓN, SISTEMA DE GESTIÓN HOSPITALARIO, SISTEMA DE GESTIÓN DEL CAMBIO.

ABSTRACT

The project grade for MGS called "IMPLEMENTATION OF A SECURE NETWORK AND HOSPITAL MANAGEMENT SYSTEM FOR HOSPITAL SPECIALTY OF ARMED FORCES" presents the implementation of a Secure Data Network, based on the ISO 17799 standard to that the Hospital Management Information System to be installed to flow through this network security, reliability , stability.

This project presents a comprehensive solution to the system of medical, administrative management of the nursing home.

Implementing a secure network based on the ISO 17799 in order to ensure a permanent and stable connectivity for a Hospital Management Information System is installed by applying a management Institutional Change international standard, will have proper control of the Medical and Administrative Management, thus achieving abide by the provisions of the Ministry of Public Health is to apply as a domestic tariff and automatically bill all services provided by the HE- 1.

Keywords: **MILITARY HOSPITAL, NETWORK SECURITY, IMPLEMENTATION, HOSPITAL MANAGEMENT SYSTEM , CHANGE MANAGEMENT SYSTEM .**

CAPÍTULO I
MARCO TEÓRICO

1.1 INTRODUCCIÓN Y ANTECEDENTES

La historia de los hospitales militares se encuentra íntimamente relacionada con la Historia de la Patria y de la Sanidad Militar, desde las luchas por la independencia hasta la actualidad, la historia se remonta a los albores del siglo XX y según datos históricos fue el 27 de diciembre de 1918 que se funda el Hospital Militar en Quito.

En décadas anteriores la sanidad militar inicia sus actividades en una de las salas del antiguo Hospital San Juan de Dios, como se indica en el gráfico 1.1, que junto al Hospital San Lázaro, eran los únicos hospitales que prestaban sus servicios en la ciudad de Quito.

Gráfico 1.1- Hospital San Juan de Dios

En este edificio, inaugurado oficialmente el 6 de enero de 1919, se crean los servicios de consulta externa. Esta época terminó cuando el servicio de consulta

externa se trasladó en 1936 al Sanatorio de San Juan, espacioso local que pertenecía en aquellos años, al Grupo de Artillería "BOLIVAR". En este espacioso edificio funcionó por algunos años el Hospital Territorial No 1 o más conocido como Hospital Militar de las Lomas de San Juan. En 1957 el Hospital Territorial No 1 pasa a depender del Estado Mayor del Comando Conjunto de FF.AA. Situación que motivó una nueva reestructuración orgánica, técnica y administrativa, direccionada desde los altos mandos militares y de su organización interna. En 1958 en el Gobierno de Camilo Ponce Enríquez, siendo Ministro de Defensa el Señor Alfonso Calderón, se hace constar en el programa de gobierno la construcción del nuevo Hospital Militar.

Pasaron algunos años en la construcción, hasta que el 28 de febrero de 1977 se inauguró el nuevo hospital de tercer nivel con el nombre de Hospital General de FF.AA. como se muestra en la figura 1.2, iniciándose así una tercera etapa en la historia.

Gráfico 1.2: Hospital General de las FFAA No 1.

Su apertura se caracterizó por la compleja estructura técnica y administrativa de un hospital de tercer nivel, por la organización de personal y recursos económicos,

lo que permitió que el país tenga un hospital del más alto nivel de referencia. Esta etapa estuvo marcada por el incremento de especialidades y sub-especialidades médico, quirúrgicas, odontológicas más diversas y por el equipamiento adecuado y moderno.

Durante el recorrido histórico de este hospital, como se muestra en el gráfico 1.3, se ha mantenido como un baluarte dentro del desarrollo de la medicina nacional, habiendo alcanzado un merecido prestigio gracias a los logros alcanzados por todo el personal que ha trabajado con responsabilidad y entrega total.

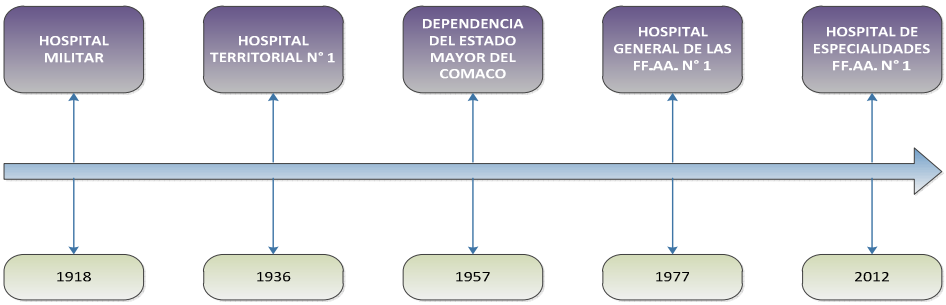


Gráfico 1.3- Línea de Tiempo de la Historia del HE-1

1.1.1 ALCANCE Y JUSTIFICACIÓN

La Constitución de la República del Ecuador en su Art. 360 manda: "…La red pública integral de salud será parte del sistema nacional de salud y están conformadas por el conjunto articulado de establecimientos estatales, de la seguridad social y con otros proveedores que pertenecen al Estado, con vínculos jurídicos, operativos y de complementariedad,".

La misma Constitución de la República en el Art. 361 ordena que: “El Estado ejercerá la rectoría del sistema a través de la autoridad sanitaria nacional, será responsable de formular la política de salud y normará, regulará y controlará todas las actividades relacionadas con la salud, así como el funcionamiento de las entidades del sector”.

La Sanidad Militar de Fuerzas Armadas se encuentra en un proceso de reestructuración y dentro de este marco se está realizando la integración del Sistema de Sanidad de las Fuerzas Terrestre, Naval y Aérea; por lo que se ve en la necesidad de implementar un sistema informático que permita optimizar la atención médica en el Hospital de Especialidades de Fuerzas Armadas, que iría en beneficio del personal militar, sus dependientes, derecho habientes y comunidad en general a nivel nacional.

Bajo este contexto, el Estado a través del registro oficial 289, dispone la aplicación del tarifario de prestaciones para el Sistema Nacional de Salud, tema de facturación, atención a pacientes del MIES, IESS, Soat, y ante estos nuevos requerimientos, el Hospital de Especialidades de FFAA no cuenta con un sistema informático, lo que se hace imperante contar con una red segura y un sistema informático de gestión hospitalario.

Hoy en día, las organizaciones y sus sistemas de redes de información se enfrentan con amenazas de seguridad procedentes de una amplia gama de fuentes, ciertas fuentes de daños como virus informáticos y ataques de intrusión se están volviendo cada vez más comunes. Las consecuencias para el HE-1 cuando ocurre un daño en la información pueden provocar pérdidas importantes, hasta el punto de afectar la continuidad del servicio de salud.

Las políticas de seguridad de la información en el Hospital de Especialidades de FFAA, son casi nulas, la información existente en esta casa de salud como: datos de los pacientes, historias clínicas, hojas de epicrisis, diagnósticos, tratamientos, turnos subsecuentes, etc. no disponen de políticas de seguridad de la red de datos, siendo una debilidad potencial para la gestión de la seguridad de la información.

Por lo anterior, es fundamental que el HE-1 gestione la seguridad de la información, de tal manera que se garantice la confidencialidad, integridad y disponibilidad de la información.

Los beneficiarios de este proyecto serán para todos los miembros de Fuerzas Armadas, sus familias, pacientes civiles y profesionales de salud que laboran en Fuerzas Armadas. Esta implementación del Sistema de Gestión Hospitalario, busca establecer una Gestión Administrativa eficiente y eficaz, así como incorporar los servicios de salud de este hospital militar, a la Red de Salud Nacional dispuesta por el Gobierno Nacional.

1.1.2 MARCO JURÍDICO

LEY ORGÁNICA DEL SISTEMA NACIONAL DE SALUD

Capítulo IV. Del Funcionamiento del Sistema.

Art. 9.-<u>Del funcionamiento</u>

El Sistema Nacional de Salud funcionará de manera descentralizada, desconcentrada y participativa; para el efecto sus integrantes se relacionarán mediante las funciones de coordinación, provisión de servicios, aseguramiento y financiamiento. ***Las instituciones que forman parte del Sistema Nacional de Salud, se articulan colaborando en el marco de sus funciones específicas y de sus***

respectivas competencias, para el cumplimiento de los mandatos previstos en esta Ley y en el Código de Salud Nacional.

ACUERDO N. 318 TIPOLOGIA PARA HOMOLOGAR LOS ESTABLECIMIENTOS DE SALUD POR NIVELES DE ATENCIÓN DEL SISTEMA NACIONAL DE SALUD.

Definiciones del IIl Nivel de Atención

Corresponde a los establecimientos que prestan servicios ambulatorios y hospitalarios de especialidad y especializados, los centros hospitalarios son de referencia nacional; resuelve los problemas de salud de alta complejidad, tiene recursos de tecnología de punta, intervención quirúrgica de alta severidad, realiza transplantes, cuidados intensivos, cuenta con subespecialidades reconocidas por la ley.

Hospital De Especialidades:

Establecimiento de salud de la más alta complejidad, que provee atención ambulatoria en consulta externa, emergencia y hospitalización en las especialidades y subespecialidades de la medicina, farmacia institucional para el establecimiento público y farmacia interna para el establecimiento privado.

Destinado a brindar atención clínico- quirúrgica en las diferentes patologías y senvicios. Atiende a la población del país a través del sistema de referencia y contra referencia; su ámbito de acción es nacional o regional.

1.1.3 MISIÓN DEL HOSPITAL DE ESPECIALIDADES FF.AA No. 1

Proporcionar atención médica integral de tercer nivel con calidad y calidez; al personal militar en apoyo a las operaciones militares y con su capacidad disponible al

personal militar en servicio pasivo, dependientes, derechohabiente y a la población civil, dentro del sistema de referencia y contra-referencia militar y nacional.

1.1.4 MODELO GRÁFICO

Este modelo describe el flujo de atribuciones de cada una de las entidades externas que se relacionan con el HE-1.

Ministerio de Salud Pública.- Emite políticas de Estado en Salud Pública que permitan recuperar las capacidades de las Unidades de Salud a través de cuatro competencias establecidas en el MSP, las cuales son: Gobernanza; Prevención y Promoción; Provisión; Vigilancia y Control. El MSP en su Modelo de Gestión además establece principios de eficiencia, participación, optimización del Talento Humano y organización para procesos de Desconcentración y Descentralización y así garantizar a través de la Prestación de Servicios de Salud una Atención de Calidad. Así pues, le corresponde al Ministerio de Defensa Nacional en coordinación con el Comando Conjunto de Fuerza Armadas ejecutar las acciones necesarias.

Ministerio de Defensa Nacional.- Las políticas desarrolladas para la gestión del Sistema Sanidad de Fuerzas Armadas, se basan en la ejecución de una de las capacidades del Plan de Capacidades al Sostenimiento Logístico referente a la Sanidad como uno de sus componentes y las medidas de gestión del Contingente, medios o recursos para el apoyo en diferentes áreas donde se encuentra Sanidad. Así se logra organizar las Unidades Militares de Sanidad en todos los niveles de atención para aplicarlas en la población militar siendo estas coordinadas y supervisadas por el Comando Conjunto de Fuerza Armadas, proporcionando atención médica a la comunidad con su personal en caso que lo requiera.

COMACO/Dirección de Sanidad de Fuerzas Armadas.- Emiten lineamientos, Normas y Directrices de Sanidad Militar, Plan Integral de Sanidad Militar y Apéndice de Sanidad para Operaciones Militares Conjuntas, basadas en la Planificación Estratégica, conducción y coordinación Institucional a través de la cual se proporcionará apoyo al Direccionamiento Estratégico de Sanidad Militar en Apoyo a las Operaciones Militares, siendo responsables de esta integración los señores Jefes del: Comando Conjunto de las Fuerzas Armadas, Planificación Militar Estratégica Operacional e Institucional, Director de Sanidad de las Fuerzas Armadas, Directores de los Centros Coordinadores de Sanidad y miembros del Sistema de Sanidad de cada Unidad de Salud (I,II,III Nivel).

Las actividades de Sanidad Militar dentro del apoyo a las operaciones militares, se constituyen en necesidades planificadas o de contingencia que deben ser ejecutadas a través de lineamientos, normas y directrices de Sanidad Militar y Salud Pública.

La responsabilidad de la emisión de las mismas será del Comando Conjunto de las Fuerzas Armadas y Sistema Sanidad de Fuerzas Armadas.

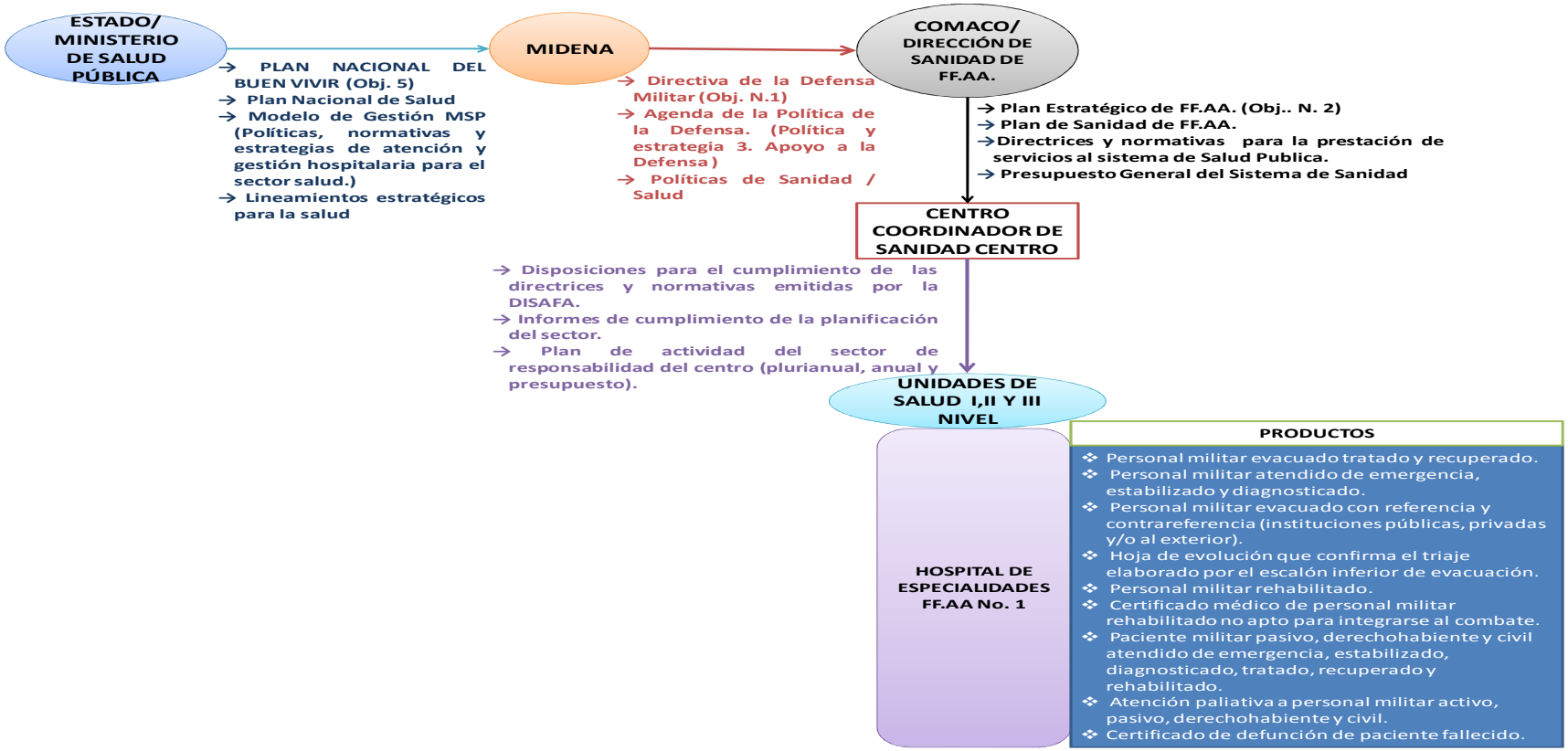
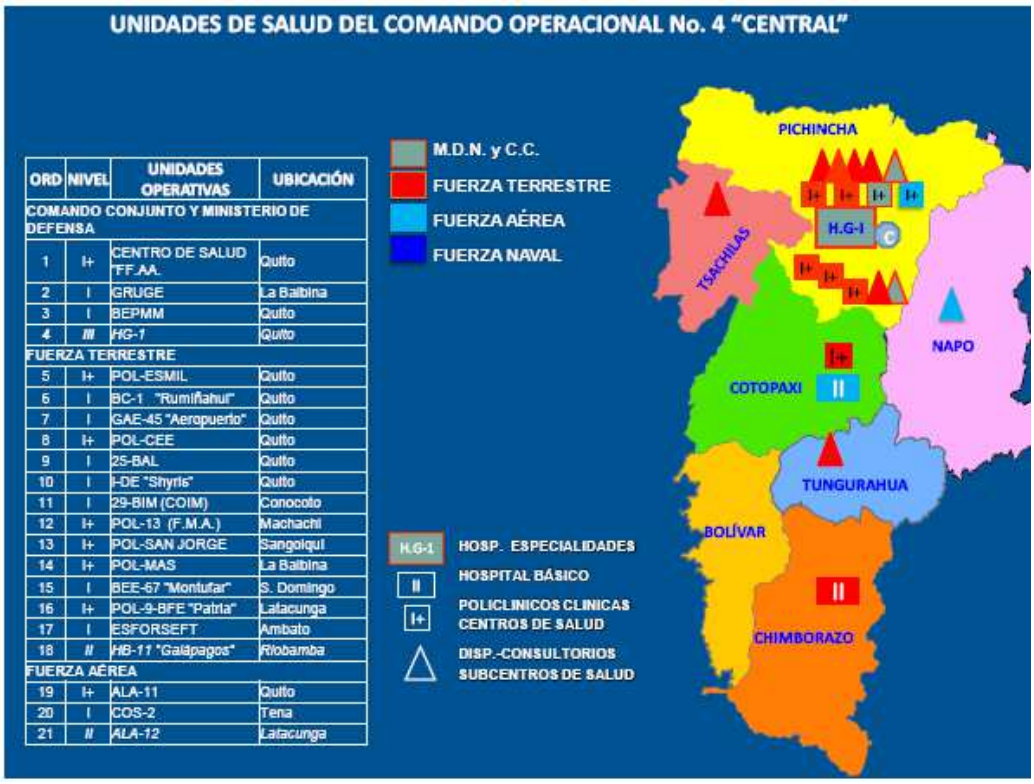


Gráfico 1.4: Flujo de atribuciones de las entidades externas que se relacionan con el HE-1.

Centro Coordinador de Sanidad.- Emite disposiciones para la ejecución de políticas, normas y directivas de sanidad militar y de salud a las Unidades de Salud de I, II y III nivel de atención en el territorio de su competencia y del cumplimiento de las mismas emitirán informes consolidados de cumplimiento de la gestión en sanidad y de salud a la Dirección de Sanidad de las Fuerzas Armadas y este a su vez remitirá al Comando Conjunto de las Fuerzas Armadas y al Ministerio de Salud Pública.

Le corresponde al Centro Coordinador de Sanidad Centro la siguiente delimitación territorial:



ORD	NIVEL	UNIDADES OPERATIVAS	UBICACIÓN
COMANDO CONJUNTO Y MINISTERIO DE DEFENSA			
1	I+	CENTRO DE SALUD "FF.AA.	Quito
2	I	GRUGE	La Balbina
3	I	BEPMM	Quito
4	III	*HG-1*	*Quito*
FUERZA TERRESTRE			
5	I+	POL-ESMIL	Quito
6	I	BC-1 "Rumiñahui"	Quito
7	I	GAE-45 "Aeropuerto"	Quito
8	I+	POL-CEE	Quito
9	I	25-BAL	Quito
10	I	I-DE "Shyris"	Quito
11	I	29-BIM (COIM)	Conocoto
12	I+	POL-13 (F.M.A.)	Machachi
13	I+	POL-SAN JORGE	Sangolquí
14	I+	POL-MAS	La Balbina
15	I	BEE-67 "Montufar"	S. Domingo
16	I+	POL-9-BFE "Patria"	Latacunga
17	I	ESFORSEFT	Ambato
18	II	*HB-11 "Galápagos"*	*Riobamba*
FUERZA AÉREA			
19	I+	ALA-11	Quito
20	I	COS-2	Tena
21	II	*ALA-12*	*Latacunga*

Gráfico 1.5: Unidades de salud del C.O. 4

Unidades de Salud I, II y III Nivel.- La Sanidad Militar proporcionará atención médica en el sitio de operaciones (móviles) e instalaciones militares (permanentes), en el ámbito de sus competencias, manteniendo al personal psicofísicamente apto para el empleo, y en forma articulada a la comunidad, siendo responsable de su cumplimiento el Comandante de la Unidad Sanitaria.

Del cumplimiento de las mismas los Comandantes de las Unidades Sanitarias emitirán a los Centros Coordinadores de Sanidad informes consolidados de la gestión de sanidad y de salud y estas a su vez remitirán los informes estadísticos a la Dirección de Sanidad del Comando Conjunto de las Fuerzas Armadas.

1.1.5 ACTORES (Unidades Administrativas u Operativas)

El Hospital de Especialidades FF.AA No. 1 se relaciona con varias entidades en el desarrollo de sus actividades las cuales son:

- El Ministerio de Salud Pública.
- Ministerio Coordinador de la Seguridad.
- Secretaría Nacional de Planificación y Desarrollo.

Los actores internos que tienen relación con el HE-1 son:

- Subsecretaría de Planificación del Ministerio de Defensa Nacional
- Estado Mayor Institucional de FF.AA (CC.FF.AA).

Gráfico 1.6: Interrelacionamiento entre cada uno de los actores internos y externos:

1.1.6 ATRIBUCIONES Y RESPONSABILIDADES

Ministerio de Defensa Nacional

- Emitir la Agenda de la Política de la Defensa Nacional.
- Políticas y directrices para la Gestión en Contingente, medio o recursos para el apoyo en el área de Sanidad.

Comando Conjunto FF.AA / Dirección de Sanidad de FF.AA.

- Emitir el Plan de Capacidades de Sostenimiento Logístico/Sanidad.
- Elaborar el Plan de Sanidad de FFAA.
- Emitir Directrices y normativas para la prestación de servicios al sistema de Salud Pública.
- Elaborar y realizar el seguimiento al Presupuesto General del Sistema.

Centro Coordinador Centro

- Emitir disposiciones para el cumplimiento de las directrices y normativas emitidas por la DISAFA.
- Elaborar informes de cumplimiento de la planificación del sector.
- Realizar un Plan de actividad del sector de responsabilidad del centro (plurianual, anual y presupuesto).

Unidad de Salud III Nivel (HE-1)

Apoyo de Sanidad a las Operaciones Militares

- Ofrecer Servicios de Salud de Tercer Nivel de mayor complejidad dentro del Sistema de Sanidad de FF.AA.
- Participar en la evacuación (transferencia) de heridos y enfermos del nivel de competencia utilizando los medios de transporte orgánicos.
- Dar tratamiento clínico, quirúrgico, rehabilitación y recuperación de los pacientes evacuados.
- Contribuir con nuestra capacidad disponible a los planes de defensa en territorio nacional y operaciones militares en apoyo a otros Organismos del Estado.

Sanidad Militar en Articulación al Sistema Nacional de Salud

- Colaborar con las Unidades del Sistema Nacional de Salud en la prestación de Servicios de Salud de Especialidad con sus competencias de Tercer Nivel.
- Prestar servicios ambulatorios y hospitalarios de especialidad (alta complejidad) de referencia y contra referencia a nivel nacional.
- Proveer atención Ambulatoria en Consulta Externa; Emergencia; UCI; Hospitalización; Farmacia Institucional; Clínico Quirúrgico. (III. 3. Hospital de Especialidades)

1.2 IMPLEMENTACIÓN DE UNA RED SEGURA

La ISO 27001 especifica los requisitos necesarios para establecer, implantar, mantener y mejorar un Sistema de Gestión de la Seguridad de la Información (SGSI)

según el conocido “Ciclo de Deming”: PDCA(NTC-ISO/IEC 17799) (Planificar, Hacer, Verificar, Actuar).

La información es un activo vital para el éxito y la continuidad del Hospital de Especialidades de FFAA. El aseguramiento de dicha información: (Confidencialidad, Integridad y Disponibilidad) de los sistemas que la procesan es, por tanto, un objetivo de primer nivel para esta Casa de Salud.

Para la adecuada gestión de la seguridad de la red, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la red hospitalaria.

1.2.1 METODOLOGÍA PROPUESTA

- Factores Críticos de Éxito:

  El apoyo existente por parte del Escalón Superior: Ministerio de Defensa Nacional, Comando Conjunto de FFAA y la Dirección General del Hospital de Especialidades de FFAA, es de gran importancia para el éxito de este proyecto.

Los beneficios del servicio hospitalario se verán reflejados en la mejoría de atención a los pacientes con una atención con calidez y eficiencia, así como también lograr disponer de un sistema de gestión integrando la parte administrativa, médica y tecnológica.

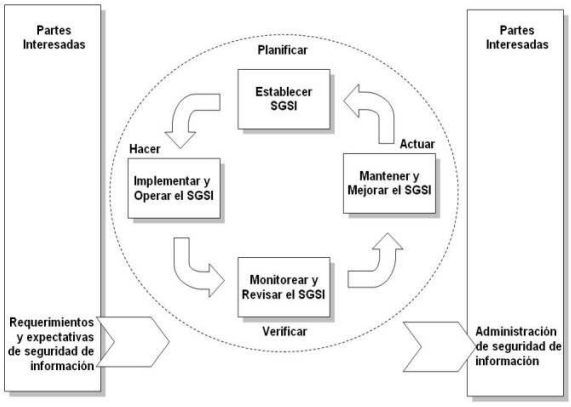


Gráfico 1.7- Proceso PHVA

1.2.1.1 PLANIFICAR

- Establecer el alcance del Sistema de Gestión de Seguridad de la Red.
- Formular las políticas de Sistema de Gestión de Seguridad de la Red.
- Ejecutar la valoración de riesgos de la red.
- Tomar decisiones en el tratamiento de riesgos.

1.2.1.2 HACER

- Crear el plan de tratamiento de riesgos.
- Implementar los controles.
- Capacitar y sensibilizar.
- Implementando un programa de manejo de incidentes de seguridad de la red.
- Administrar recursos de la red.

1.2.1.3 VERIFICAR

- Monitorear
- Hacer Auditorías internas del Sistema de Gestión de Seguridad de la Red
- Ejecutar revisiones administrativas
- Medir el Sistema de Gestión de Seguridad de la Red
- Analizar tendencias
- Controlar documentación y registros.

1.2.1.4 ACTUAR

- Implementar mejoras
- Identificar no-conformidades
- Identificar e implementar acciones preventivas y correctivas
- Asegurar la mejora continua.
- Probar
- Comunicar cambios y mejoras

Lo que se plantea con esta metodología para este proyecto es planificar la implementación de una red segura formulando políticas de seguridad para salvaguardar la información, siendo uno de los bienes más preciados sobre todo Por ser un servicio de salud donde se pone en juego la vida de los seres humanos.

Los grados de riesgos existentes los podemos identificar como bajos, medios y altos y los riesgos existentes a que se muestra la información en esta casa de salud son: la pérdida de información por distintos factores externos o internos, mala manipulación por parte de los usuarios de la red hospitalaria, ataques informáticos,

virus, red eléctrica, etc. La forma en que se opere, se verifique y se actúe con políticas, controles, procesos y procedimientos, para analizar y medir los procesos relacionados al Sistema de Gestión de la Seguridad de la Información, evaluar objetivos, experiencias e informar los resultados para su revisión y tomar acciones preventivas y correctivas basadas en controles internos que se realizan en esta casa de salud, son las acciones que permitirán garantizar una red segura.

1.2.2 NORMA ISO 17799

La Norma ISO 17799 es un conjunto de controles que incluyen las "mejores prácticas" en seguridad de la información, cuya principal intención es servir como un punto de referencia único para identificar los controles necesarios en la mayoría de las situaciones en los que los sistemas de información se ven involucrados.

- ***Confidencialidad***: sólo el personal o equipos autorizados pueden acceder a la información.
- ***Integrida****d:* la información y sus métodos de proceso son exactos y completos.
- ***Disponibilidad*****:** los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando se requieran.

La norma UNE-ISO/IEC 17799 establece **diez dominios de control** que cubren por completo la Gestión de la Seguridad de la Información

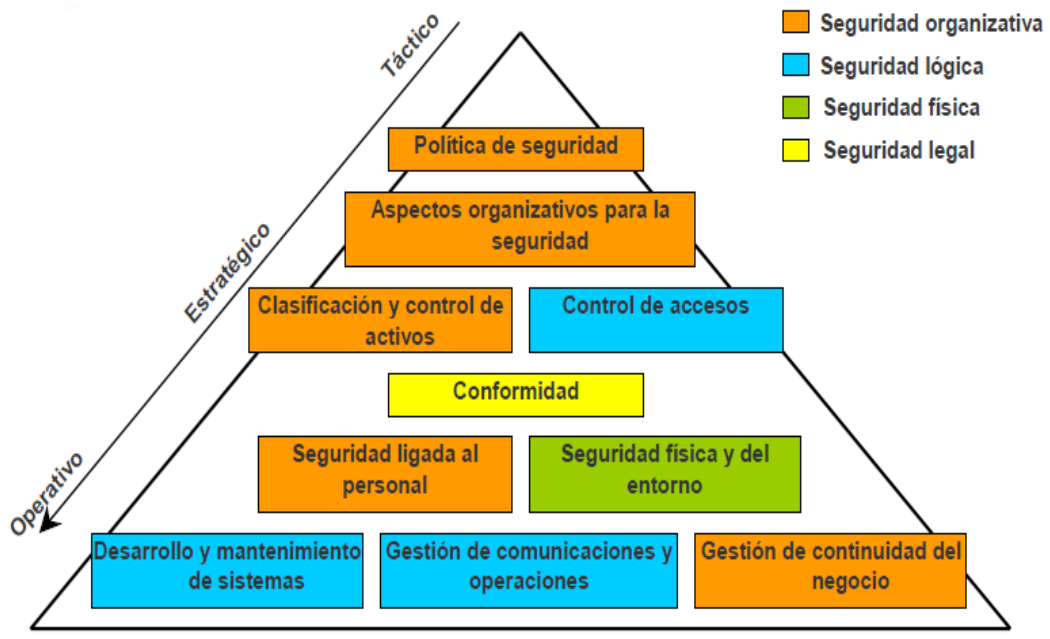


Gráfico 1.8: Pilares de la seguridad ISO 17799

Dominios de Control:

1. **Política de seguridad:**

- La Dirección General del HE-1 debe definir una política que refleje la línea directriz en materia de seguridad, aprobarla y publicitarla de la forma adecuada a todo el personal implicado en la seguridad de la red.
- Esta política se debe constituir en la base de todo el sistema de seguridad de la red, en donde la alta dirección debe apoyar visiblemente la seguridad de la red de datos en el HE-1.

2. **Aspectos organizativos para la seguridad.**

- Gestionar la seguridad de la red de datos dentro del HE-1, mantener la seguridad

de los recursos de tratamiento de la información y de los activos de red de la organización que son accedidos por terceros.

- Diseñar una estructura organizativa dentro del HE-1, que defina las responsabilidades que en materia de seguridad que tiene cada usuario o área de trabajo relacionado con la red de datos de cualquier forma, con un enfoque multidisciplinario, los problemas de seguridad no son exclusivamente técnicos.

3. Clasificación y control de activos.

- Mantener una protección adecuada sobre los equipos activos de red del HE-1, asegurar un nivel de protección adecuado.
- Debe definirse una clasificación de los activos relacionados con la red de datos, manteniendo un inventario actualizado que registre estos datos, y proporcionando a cada activo el nivel de protección adecuado a su criticidad.

4. Seguridad ligada al personal.

- Reducir los riesgos de errores humanos, robos, fraudes o mal uso de las instalaciones y los servicios hospitalarios.
- Asegurar que los usuarios sean conscientes de las amenazas y riesgos en el ámbito de la seguridad de la red, y que estén preparados para sostener la política de seguridad de la red del HE-1en el curso normal de su trabajo.
- Minimizar los daños provocados por incidencias de seguridad y por el mal funcionamiento, controlándolos y aprendiendo de ellos.

- Las implicaciones del factor humano en la seguridad de la información son muy elevadas. Todo el personal, tanto interno comoexterno del hospital, debe conocer tanto las líneas generales de la política de seguridad de la red como las implicaciones de su trabajo en el mantenimiento de la seguridad global.
- Diferentes relaciones con los sistemas de información: operador, administrador, guardia de seguridad, personal de servicios, etc.

5. Seguridad física y del entorno.

- Evitar accesos no autorizados, daños e interferencias contra la infraestructura de red y la información del HE-1.
- Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades hospitalarias.
- Prevenir las exposiciones a riesgo o robos de la infraestructura de red.
- Las áreas de trabajo técnico del HE-1 deben ser clasificadas y protegidas en función de su criticidad, siempre de una forma adecuada y frente a cualquier riesgo factible de índole física (robo, inundación, incendio...).

6. Gestión de comunicaciones y operaciones.

- Asegurar la operación correcta y segura de los recursos de la red.
- Minimizar el riesgo de fallos en la red.
- Proteger la integridad del software y de la información de red.
- Mantener la integridad y la disponibilidad de los servicios de red.

- Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo.
- Prevenir la pérdida, modificación o mal uso de la información intercambiada entre la red de salud nacional.
- Se debe garantizar la seguridad de las comunicaciones y de la operación de los sistemas críticos para los servicios hospitalarios.

7. Control de accesos.

Se deben establecer los **controles de acceso adecuados** para proteger el área del centro de datos del HE-1, sistema operativo, aplicaciones, redes, etc.

8. Desarrollo y mantenimiento de sistemas.

Debe contemplarse la seguridad de la información en todas las etapas del ciclo de vida del software: especificación de requisitos, desarrollo, explotación, mantenimiento.

9. Gestión de continuidad del negocio.

- Todas las situaciones que puedan provocar la interrupción de las actividades hospitalarias deben ser prevenidas y contrarrestadas mediante los planes de contingencia adecuados.
- Los planes de contingencia deben ser probados y revisados periódicamente.
- Se deben definir equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

10. Conformidad con la legislación.

- Se debe identificar convenientemente la legislación aplicable a los sistemas de información corporativos, integrándola en el sistema de seguridad de la información de la compañía y garantizando su cumplimiento.
- Se debe definir un plan de auditoría interna y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.
- En este proyecto no aplica los pilares 8,9 y 10; por estar orientado la seguridad a la red de datos como tal y no a la información de manera generalizada.

1.3 SISTEMA DE GESTIÓN HOSPITALARIO

1.3.1 MODELO DE GESTIÓN

1.3.1.1 OBJETIVOS DEL MODELO DE GESTIÓN

Objetivo general:

Proporcionar un esquema de administración que permita desarrollar políticas y acciones para el cumplimiento de los objetivos institucionales.

Objetivos específicos:

- Asegurar el apoyo de sanidad a las operaciones militares, mediante la ejecución de políticas de atención prioritaria para personal militar en servicio activo, con el fin de garantizar la integridad del personal.

- Desarrollar equipos multidisciplinarios técnicos–administrativos en base a las competencias establecidas, para potencializar los recursos disponibles financieros, de infraestructura y equipamiento médico.
- Ejecutar las políticas de salud de referencia y contra-referencia establecidas por el Sistema Nacional de Salud, mediante la racionalización de la atención médica, para satisfacer la demanda de servicios de salud de tercer nivel de especialidad.
- Fortalecer la capacitación técnica, mediante el acceso y la participación de estudios en línea, con la finalidad de actualizar los conocimientos de manera continua en nuevas prácticas.
- Generar una cultura organizacional por procesos a través del involucramiento del talento humano del HE-1

1.3.1.2 PROCESOS, SUBPROCESOS Y PRODUCTOS/SERVICIOS.

Mapa de procesos

Diagrama que permite identificar los macro procesos de esta casa de salud por su tipo y describe sus interrelaciones principales. Los tipos de macro procesos que se describen en el mapa de procesos son: procesos gobernantes, procesos sustantivos y procesos adjetivos.

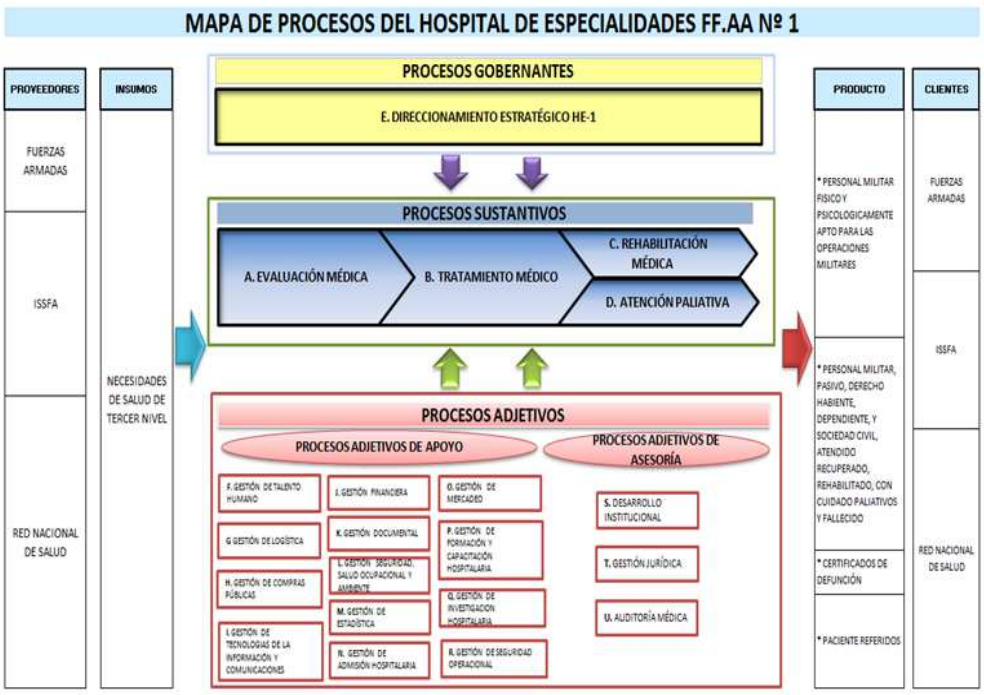


Gráfico 1.9: Mapa de procesos

Tabla 1.1: Despliegue de Procesos

MACRO PROCESO	PROCESOS
A. EVALUACIÓN MÉDICA	A1. EVALUACIÓN DE ENFERMERÍA
	A.2 EVALUACIÓN CLÍNICA QUIRÚRGICA
	A.3 EXÁMENES COMPLEMENTARIOS
	A.4 VALORACIÓN MÉDICA INTEGRAL
B. TRATAMIENTO MÉDICO	B.1 ATENCIÓN DE ENFEREMERÍA
	B.2 ATENCIÓN MÉDICA DE TRATAMIENTO
	B.3 PROCESAQMIENTOS DE TRATAMIENTO
	B.4 EGRESO DE ATENCIÓN MÉDICA
	B.5 ATENCIÓN MÉDICA SUBSECUENTE DE CONTROL
C. REHABILITACIÓN MÉDICA	C.1 ATENCIÓN MÉDICA INTEGRAL
	C.2 REHABILITACIÓN

	C.3 INDUCCIÓN AL PACIENTE Y/O FAMILIAR
	C.4 ALTA MÉDICA
D. ATENCIÓN PALIATIVA	D.1 ATENCIÓN DE ENFEREMERÍA
	D.2 EVALUACIÓN MÉDICA PSICOLÓGICA Y ESPIRITUAL
	D.3 TRATAMIENTO, SEGUIMIENTO Y CONTROL MÉDICO, PSICOLÓGICO.
	D.4 EGRESO HOSPITALARIO PARA EL CONTROL DOMICILIARIO
	D.5 VISITA DOMICILIARIA

El Sistema Informático de Gestión Hospitalaria apoya de manera directa a los procesos de: Evaluación Médica, Tratamiento Médico, Rehabilitación Médica y Atención Paliativa, con todos sus módulos obteniendo los productos indicados.

1.3.1.3 ESTRUCTURA ORGANIZACIONAL POR PROCESOS.

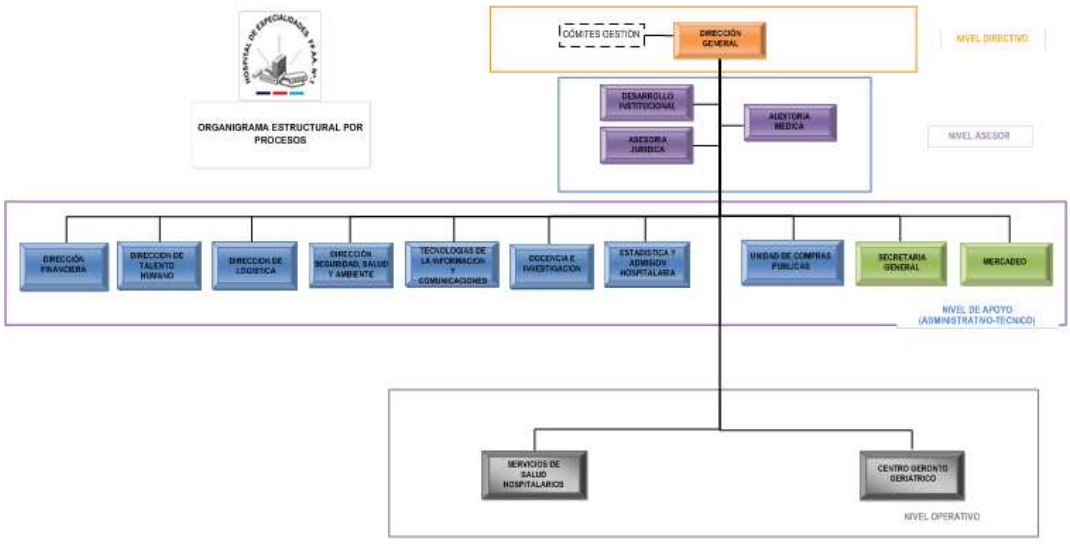


Gráfico 1.10: Estructura organizacional por procesos

1.4 GESTIÓN DEL CAMBIO

El nuevo sistema de Gestión Hospitalario, va a generar un gran impacto institucional, en donde implican valores, personas, cultura y capacidad gerencial, influencias de condicionantes internos y externos; en donde se enfrenta gran resistencia y obstáculos; ante tal complejidad, para definir el hospital del mañana se requiere de:

- Un proceso permanente de escucha (información) y reflexión (retroalimentación);
- Un pensamiento y propuesta estratégica compartida (sentido o razón de ser);
- Un liderazgo que conduzca el cambio;
- Un plan compartido (participación organizada y corresponsable).

Los elementos de complejidad planteados se integran y abordan mediante el pensamiento estratégico que es la tarea intencionada por medio de la cual el HE-1 llegue a las definiciones de nivel superior que la guiarán hacia sus objetivos, en la forma en que intentará relacionarse con el ambiente y asignar los recursos para su acción. Para que los cambios se produzcan, junto a una visión de futuro, se requiere de un grupo multidisciplinario de personas capaces de orientar, catalizar y sistematizar dichos cambios.

Se ha identificado como básico contar con los conocimientos y habilidades, con el apoyo institucional, con la capacidad de comunicar, comprometer, hacer responsable y evaluar el proceso por parte del equipo técnico multidisciplinario del HE-1.

Desarrollar una gestión que, escuche y comprenda los fenómenos que conforman el entorno del hospital, saber identificar y proyectar a las necesidades de los usuarios, quienes exigen respuestas crecientemente flexibles, oportunas, efectivas y eficientes.

Es así, que el hospital necesita desarrollar la capacidad estratégica para cambiar el Sistema Informático de Gestión Hospitalario; por lo tanto, lo crítico para este cambio es la habilidad para aprender a cambiar, o lo que es lo mismo: la capacidad institucional para aprender a escuchar, comprender, adaptarse y desarrollarse.

En un cambio institucional están implicados valores, personas, cultura y liderazgo; se recibe influencias de condicionantes internos y externos; se enfrenta resistencia y obstáculos; hay luchas de poder entre los distintos grupos internos y externos involucrados o afectados que modulan los avances y retrocesos, como también hay aciertos y errores en tácticas o estrategias, a los que hay que estar dispuesto a encontrarse en el camino del cambio.

A través de un proceso estratégico, el equipo directivo puede elaborar planes y metas específicas para mantener la ruta en la "gestión del cambio"; ante las eventualidades y los imprevistos, hacer la evaluación de riesgos y poder evaluar y señalar los resultados para ir retroalimentando y modulando el ritmo del proceso es sumamente importante. Cerrar brechas o avanzar hacia la realización de la imagen deseada implica decisiones estratégicas, que modifican en alguna forma la naturaleza del hospital.

Constituyen oportunidades para el cambio, situaciones como la implementación de un nuevo sistema informático de gestión hospitalario, un nuevo servicio, inter consultas

médicas, la ampliación de la cobertura, la adopción de nuevas formas de atención en los servicios de emergencia por ejemplo, son nuevos retos planteados.

Estas decisiones pueden plantear tareas de envergadura al hospital, pues repercuten sobre muchas de las funciones y rutinas anteriores; por ejemplo, las relaciones con procesos diferentes, nuevas prácticas, la asignación de recursos, las habilidades y conocimientos de trabajadores de salud, administrativos y técnicos.

El desafío impostergable de este tiempo es avanzar a la excelencia institucional en salud pública;

Esperar avanzar sistemática y consistentemente a establecimientos hospitalarios de clase mundial hacia fines de la presente década.

1.4.1 EL CAMBIO DE LA CULTURA INSTITUCIONAL

La cultura hospitalaria es el conjunto de referencias compartidas entre todos los participantes, como resultado de una historia y de significados comunes que se dan a las situaciones y a las relaciones mediante el diario vivir, la cultura se forja y modifica en las relaciones de cotidianeidad del hospital.

Los procesos de cambio en organizaciones de salud, no pueden entenderse sino como proceso de cambio de cultura, de cómo las personas se replantean valores y conductas en su quehacer y relaciones diarias sobre todo al personal militar en retiro y sus dependientes que son la mayoría de usuarios del hospital militar.

Los elementos críticos de la cultura organizacional, con relación a un proceso de cambios, son la desconfianza existente en el personal de médicos, enfermeras y administrativos que generan rumores, de conversaciones subterráneas que nunca se expresan abierta y formalmente, son factores muy importantes a ser analizados y montar

una estrategia que pueda desarmar este desanimo que puede incidir en el éxito de la implementación del sistema de gestión hospitalaria.

Lo habitual de la cultura hospitalaria tradicional es su apego al statu quo, el mayor desafío será mover esa cultura a una que valore por sobre todo el desarrollo de capacidades continuas de aprendizaje y de validación de los procesos en relación a evidencia. Una frase nefasta en los establecimientos hospitalarios, y que debiera ser transmutada es “siempre se ha hecho así”.

La cultura tiene que ver con la comprensión y el cuidado del ambiente laboral, esta es la dimensión de la que muchas veces no se habla pero en la cual se encuentran los principales factores que afectan todo proceso de cambio cultural. El clima hospitalario influye en la motivación de las personas, el desempeño, la satisfacción, son demandantes.

Se hace fundamental, antes de iniciar cualquier proceso de cambios, “escuchar” y permear la cultura. Cada hospital posee su propia cultura; sus tradiciones y métodos de acción que en conjunto definen el clima del hospital. El clima hospitalario es el ambiente humano dentro del cual realizan su trabajo.

Una de las formas efectivas de permear la cultura es desplegar al máximo en el hospital la información y la participación; los fundamentos de las decisiones tomadas deben ser explicitados, socializados “hasta el cansancio” por los líderes, sobre todo en personas hostiles al cambio y, mejor aún, los procesos de toma de decisiones deben ser participativos, con todos los actores involucrados representados, en espacios de trabajo multiestamentarios.

1.4.2 LA FUNCIÓN DE LA DIRECCIÓN EN LA CONDUCCIÓN DEL CAMBIO.

Cuando un grupo humano tiene la oportunidad de vivir la confluencia de un buen líder, de una misión titánica construida desde los valores de las personas y de un plan de acción compartido, está en medio de una oportunidad de cambio organizacional.

El director y, mejor aún, el equipo directivo, es un grupo - líder multidisciplinario, que debe movilizar al hospital en el cumplimiento de su función, la cual debe ser incorporada en carácter de misión institucional y traducida a objetivos estratégicos precisos y verificables.

Para el cumplimiento efectivo de su misión, el equipo directivo debe comprometer a todo el hospital para que, repensándose constantemente a sí misma, responda efectivamente a las necesidades de salud requeridas; se adapte con éxito a las nuevas condiciones procesos, políticas del medio; cumpla con los objetivos de producción requeridos por los servicios hospitalarios; se posicione adecuadamente el nuevo sistema; y dé cuenta ante los entes participativos y los organismos públicos pertinentes (políticos y de financiamiento) de los resultados obtenidos con los recursos disponibles.

Todo proceso de cambios implica riesgos, desde equivocaciones incidentales hasta errores que pueden dificultar seriamente la marcha del proceso. Nada más útil ante ello, que mantener los canales de participación ya mencionados, y usarlos para la autocrítica y para transparentar con humildad y franqueza tanto los éxitos, como las dificultades y los errores.

1.4.3 LA RESISTENCIA AL CAMBIO

La resistencia al cambio es una reacción humana normal que se debe tener en cuenta siempre que se pretende hacer cambios, los tiempos en que los cambios eran violentamente impuestos por las autoridades ya pasaron, la experiencia señala que basta que se retire la fuerza que impuso los cambios para que vuelvan “las viejas conductas”.

El grupo técnico multidisciplinario del hospital, al gestionar la resistencia, debe ocuparse de cuatro dimensiones del cambio: personal, interpersonal, gerencial y organizacional. Tienen que “enseñar” a aprender y a creer en los desafíos, ya que las personas son capaces de hacer grandes cosas cuando piensan en grandes cosas. Es decir, “somos lo que pensamos que somos”. La clave de las técnicas que se utilicen para desencadenar el proceso estará en cuán exitosas sean en convocar a un pensamiento “común” de un nuevo establecimiento.

El Hospital Militar registra algunas oportunidades fallidas de implementaciones de un nuevo software hospitalario, no es raro encontrarse con que en oportunidades se ha decidido instalar un cambio, se ha hecho todo lo necesario, pero el cambio no funciona y no es practicado. Los síntomas que evidencian las oportunidades fallidas son:

- La innovación fue tácitamente aceptada, pero no está siendo usada.
- Existe indiferencia por parte de algunas personas o grupos completos.
- Se manifiestan contra argumentaciones sin ninguna base real.
- Las innovaciones son ridiculizadas, como faltas de sentido e inteligencia.
- Existe un marcado esfuerzo por anular los efectos del cambio.
- La implantación de la innovación se dilata sin motivo alguno.

Estos síntomas son generados por algunos motivos que a la postre son los que se deben identificar y eliminar para minimizar la resistencia al cambio.

Cualquier intervención en un proceso, sea de orden técnico, organizacional o administrativo implica un cambio social, esto es, que al innovar se crea una amenaza a la continuidad de las relaciones existentes entre los individuos que se verán afectados. La cultura social es un conjunto de actividades y hábitos aprendidos que relacionan a un grupo de personas y hacen que se valore de diferente forma cualquier conducta o acción. Por su parte, los individuos resisten a las innovaciones por:

- Ansiedades e inseguridades:
- Temor de asumir riesgos con los cuales no están familiarizados
- Temor a tornarse prescindible en su cargo por efecto del cambio
- Temor de no ser capaz de desarrollar las nuevas funciones
- Incapacidad o falta de disposición.

1.4.4 COMO INSTALAR CAMBIOS CON RESISTENCIA

Lo primero es hacer un diagnóstico en el hospital, de los puntos que tienden a producir resistencia y luego estructurar un proceso con sus actividades bien definidas. En el diagnóstico, hay que considerar:

- ¿Cuál es el tiempo que se tiene para completar el cambio?
- ¿Cuál es la intensidad de perturbación social y cultural que se creará?
- ¿Quiénes serán afectados por el cambio?
- ¿Quiénes serán los grupos o individuos que apoyarán o resistirán el cambio?
- ¿Cuáles serán los motivos para apoyar o resistir el cambio?

- ¿Cuál será la importancia relativa de estos individuos o grupos para el éxito del cambio?

Una vez estudiado y diagnosticado el efecto del cambio, se sugiere las siguientes medidas o técnicas para gestionar la resistencia:

Transparencia: Informar a toda la organización, tratando de reducir temores y ansiedades. Si se han detectado personas o grupos de mayor resistencia, hay que dedicar mayor atención a éstos.

Participación: Involucrando a las personas que serán directamente afectadas en el planeamiento y el contenido del cambio, con lo que se logrará disminuir la resistencia. Las personas tienden a dar apoyo a lo que han ayudado a crear.

Educación y entrenamiento: Es imperativo entrenar a los afectados, ya que cualquier cambiosignifica olvidar hábitos y adquirir nuevos, aún más, los involucrados en el cambio deberán adquirir nuevas experiencias y olvidar experiencias pasadas, esto es lo que hemos definido como capacitación estratégica (aprender a aprender).

Tiempo: Se vio que la resistencia al cambio es mayor si se pretende hacer en un corto plazo y disminuye si el cambio es hecho en plazos mayores. Si se estima que el tiempo es escaso, se requerirá una estructura de poder reforzada, y si es necesario habrá que reforzar este poder antes de efectuar el cambio, ya que un cambio fallido es doblemente resistido en un segundo intento.

Secuencia: Los cambios se pueden hacer en grupos piloto, con la ventaja de poder elegir grupos de baja resistencia, analizar los efectos, corregir y mejorar procesos; si el cambio es exitoso, puede esperarse un efecto de contagio ya que cuando otros grupos o individuos se percatan del éxito querrán imitar.Instalar los cambios por servicios o por

pisos en el edificio de hospitalización, es decir en partes para ir completando el cambio en forma gradual es otra forma de enfrentar estratégicamente el proceso.

Aplicación de técnicas de desarrollo institucional: El logro de cambios exitosos y sustentables, requiere de la utilización de técnicas modernas de desarrollo organizacional, desde la planeación estratégica; el mapeo de actores; técnicas de manejo de conflictos. Es clave comprender que cambios complejos no pueden acometerse de forma “amateur” y deberán buscarse las competencias y apoyo necesario.

C A P Í T U L O II:

SITUACIÓN TECNOLÓGICA ACTUAL DEL HE-1

2.1 SITUACIÓN ESTRUCTURAL DE LAS TIC´s.

El modelo define un Sistema de Tecnologías de la Información y Comunicaciones que comprende la planificación institucional y su empleo de las TIC's a través de un desarrollo, administración y mantenimiento técnico de los mismos para apoyar a toda la gestión hospitalaria y administrativa, el cual fomenta la propiedad de los procesos, definiendo en cada nivel la responsabilidad dentro de la estructura del Hospital de Especialidades, con una nueva cultura de gestión Institucional direccionando, administrando y controlando la entrega de soluciones, servicios y recursos.

2.1.1. MISION DEL DTIC DEL HE-1.

"Proveer de los medios para satisfacerlas necesidades de Sistemas de Información y Comunicaciones del Hospital de Especialidades de Fuerzas Armadas N.1 a través del uso de plataformas tecnológicas de punta, para establecer una interrelación de las diferentes áreas y servicios a fin de lograr la eficiencia y eficacia en la atención al cliente, externo

2.1.2. CADENA DE VALOR

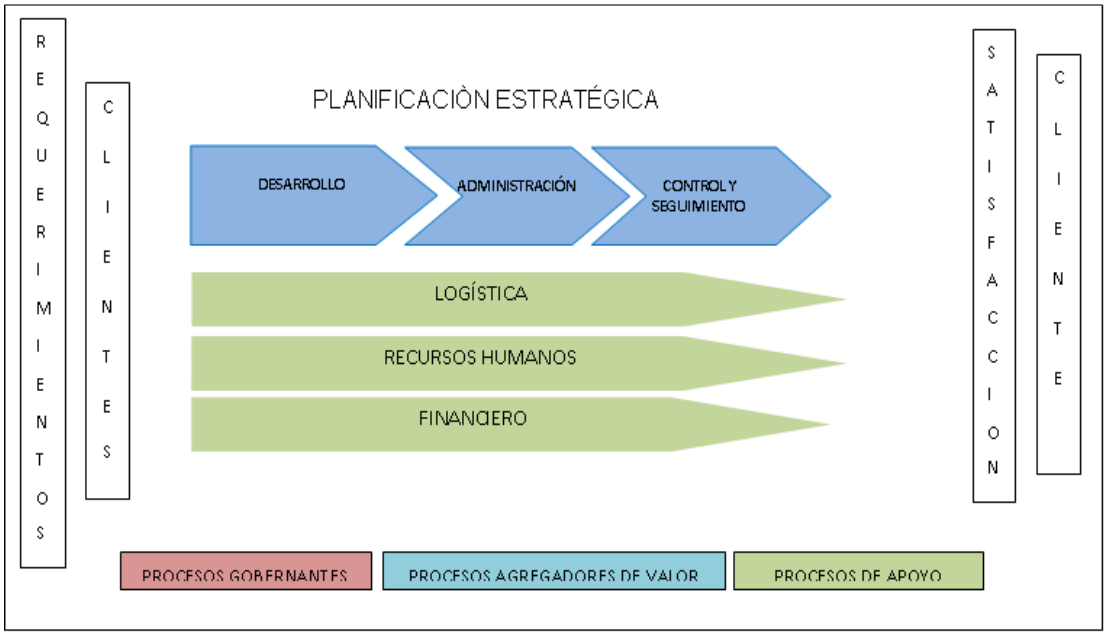


Gráfico 2.1: Cadena del Valor

2.1.3. Estructura orgánica del Departamento de Tecnologías de Información y **comunicaciones.**

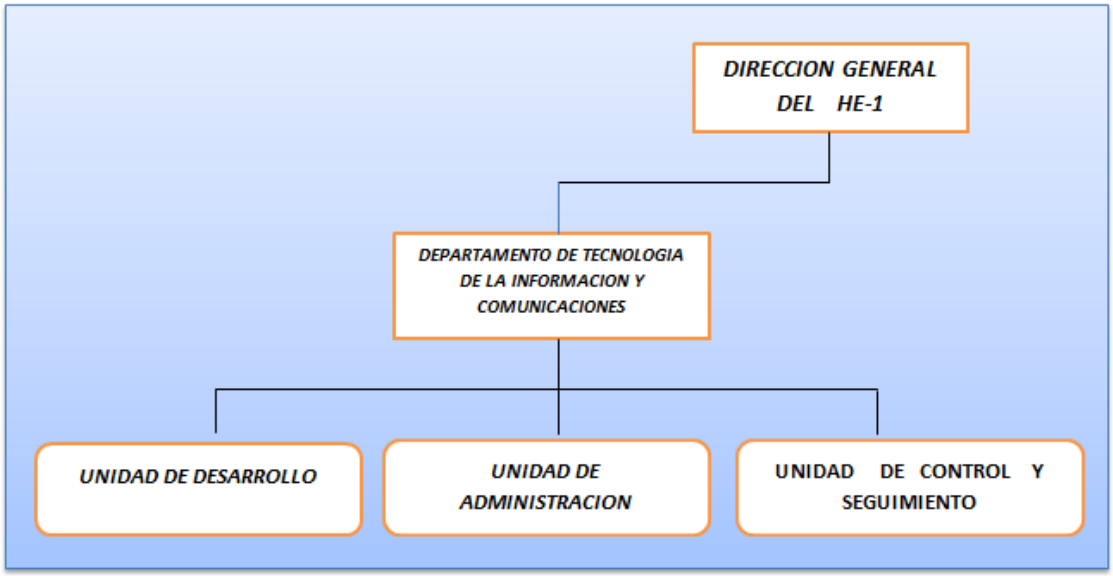


Gráfico 2.2: Estructura Orgánica del DTIC del HE-1

2.2. SITUACIÓN ACTUAL TECNOLÓGICA INFORMÁTICA DEL HE-1

2.2.1. DIAGNÓSTICO DE LA RED ACTUAL EN BASE A LOS PILARES DE LA SEGURIDAD ISO 17799

2.2.1.1 POLÍTICA DE SEGURIDAD:

La Dirección General del HE-1 no ha definido un documento con una política clara, no existe una definición de la seguridad de la red de datos y sus objetivos globales, el alcance de la seguridad y su importancia, así como políticas de seguridad, principios, normas y requisitos de cumplimiento, definición de responsabilidades generales y especificas en materia de gestión de la seguridad de la red.

La dirección debe brindar evidencia de su compromiso con esta casa de salud, mediante el:

- Establecimiento de una política de seguridad de la red de informática.
- Asegurar que se establezcan los objetivos y planes de seguridad de la red informática..
- Establecer funciones y responsabilidades de seguridad de la red informática.

Esta política debe comunicarse a todos los usuarios del HE-1, de una forma apropiada accesible y entendible.

2.2.1.2 SEGURIDAD ORGANIZACIONAL

Actualmente el HE-1 dispone contratos anuales con empresas que da soporte al hardware y software, por lo que requieren acceso físico al data center, centro de cómputo y también acceso lógico a la base de datos, servidores y al sistema de gestión hospitalario, pero no se realiza una evaluación del riesgo para determinar sus

implicaciones sobre la seguridad y definir las medidas de control que se requieren, estas medidas de control deberían definirse y aceptarse en un contrato, con la empresa correspondiente.

Existe vulnerabilidades con personal de: consultores, mantenimiento de limpieza, estudiantes que realizan prácticas en el departamento de sistemas, por lo que se necesita administrar el acceso de estas terceras partes a los recursos de procesamiento de información.

No se dispone de un contrato que gestiones y controle la administración de la base de datos, la administración de red, gestión y control del sistema informático de gestión hospitalaria.

- **Estructura para la seguridad de la red.**

  Asignación de responsabilidades para la seguridad de la red informática: se debe definir claramente las responsabilidades para la protección de los activos individuales y para realizar procesos de seguridad específicos en la red.

- **Seguridad del acceso por terceras partes.**
  - Identificación de riesgos por el acceso de terceras partes.
  - Requisitos de seguridad en contratos con terceras partes.

- **Contratación externa (Outsourcing).**

  Requisitos de seguridad en contratos de contratación externa.

2.2.1.3 CLASIFICACIÓN Y CONTROL DE ACTIVOS

El HE-1 no dispone de un inventario de activos de la infraestructura de la red de datos de manera particular para el Departamento técnico.

- **Responsabilidad sobre los activos.**
  - Activos de información: archivos y base de datos, documentación del sistema de gestión hospitalario, manuales de usuario.
  - Activos de software: Software de aplicación, herramientas y programas de desarrollo.
  - Activos físicos: Equipamiento informático (Computadoras de escritorio, computadoras portátiles, impresoras, equipos activos de red).

2.2.1.4 SEGURIDAD LIGADA AL PERSONAL

No hay una inclusión de la seguridad en las responsabilidades laborales, no ha existido una selección y política sobre el personal, ni acuerdos de confidencialidad.

No hay disponibilidad de referencias satisfactorias del personal, confirmación de las certificaciones académicas y profesionales, no se ha realizado un análisis del estado financiero del personal que ocupa puestos de alta responsabilidad en la administración de la red como tal, y en el departamento técnico.

Existe personal contratado temporalmente, no se conoce que circunstancias privadas del personal pueden afectar su trabajo, los problemas personales o financieros, los cambios de su comportamiento o estilo de vida, las ausencias recurrentes y la depresión o el estrés evidentes podrían llevar a fraudes, robos, errores u otras implicaciones de seguridad. Esta información debería manejarse de acuerdo con la legislación correspondiente.

Las implicaciones del factor humano en la seguridad de la red son muy elevadas. Todo el personal técnico del hospital, debe conocer tanto las líneas generales de la política de seguridad de la red como las implicaciones de su trabajo en esta.

- **Seguridad en la definición de cargos y suministros de recursos.**
  - **Selección y política sobre personal**

    En el momento en que se reciben las solicitudes de trabajo se deben establecer controles como referencias satisfactorias laborales y personales.

    Comprobación de la precisión de la hoja de vida del candidato.

    Confirmación de las certificaciones académicas y profesionales.
  - **Acuerdo de confidencialidad**

    Los empleados deberían firmar normalmente un acuerdo de confidencialidad o no divulgación de la información referente a base de datos, configuraciones de servidores, administración y operación del Sistema de Gestión Hospitalario, como parte de sus términos o condiciones iníciales de trabajo.
  - **Términos y condiciones de la relación laboral.**

    Se debe indicar la responsabilidad de los empleados en cuanto a la seguridad de la información, se debe incluir que hacer si el empleado incumple los requisitos de seguridad.
- **Respuestas a incidentes y anomalías en materia de seguridad de la red.**
  - No existen reportes de los incidentes de seguridad de la red.
  - No existen reportes de las anomalías del software.

- No existe un proceso disciplinario para los empleados que violen las políticas y procedimientos de seguridad de la red del hospital.

2.2.1.5 SEGURIDAD FÍSICA Y DEL ENTORNO.

No existe una protección física en torno a las instalaciones de procesamiento de la información como el centro de datos, las mismas que deberían estar protegidas con controles de entrada apropiados que aseguren que solo se permite el acceso a personal autorizado. Los equipos como servidores, base de datos no están bien ubicados y protegidos para reducir los riesgos de amenazas o peligros del entorno como inundaciones.

Falta actualizar las medidas para minimizar robos, incendios, no se monitorea las condiciones físicas y ambientales que puedan afectar negativamente el funcionamiento de los equipos activos de red.

No existe un sistema de alimentación ininterrumpida para toda la infraestructura de red. Las áreas de trabajo del HE-1y sus activos deben ser clasificadas y protegidas en función de su criticidad, siempre de una forma adecuaday frente a cualquier riesgo factible de índole física (robo, inundación, incendio...).

- **Áreas seguras.**
  - Implementar controles de acceso físico
  - Seguridad de oficinas
- **Seguridad de los equipos.**
  - Ubicación y protección de los equipos.
  - Suministro de energía.

- Seguridad del cableado.
- Mantenimiento de los equipos.

2.2.1.6 GESTIÓN DE REDES

No existen procedimientos para la gestión y operación de la infraestructura de la red, estos documentos se deben tratar como documentos formales, y sus cambios deberían autorizarse por la jefatura de las DTIC.

- **Procedimientos operacionales y responsabilidades.**
  - Procedimientos de operación de la red documentados.
  - Control de los cambios operacionales en la red.
  - Procedimientos para administración de incidentes de la red.
- **Mantenimiento interno.**
  - Información de respaldo de configuraciones de los equipos activos de red.
  - Información de respaldo de diagramas del Cableado Estructurado
  - Bitácoras del operador, cambios de configuraciones, fallas.
- **Administración de redes.**
  - Controles de redes

2.2.1.7 CONTROL DE ACCESOS

El hospital dispone de controles para el acceso a la red informática, pero no se lleva un registro adecuado.

Se deben establecer los **controles de acceso adecuados de los usuarios de la red** para proteger los sistemas de información críticos que se encuentran sobre la red informática

hospitalaria, a diferentes niveles: sistema operativo, aplicaciones, redes. Se debe desarrollar:

- **Administración de accesos de usuarios de la red.**
  - Registro de usuarios.
  - Administración de privilegios.
  - Administración de contraseñas.
  - Revisión de los derechos de acceso de los usuarios.

- **Responsabilidad de los usuarios.**
  - Uso de contraseñas.
- **Control de accesos a redes.**
  - Política de uso de los servicios de red.
  - Autenticación de usuarios para conexiones externas.
  - Autenticación de nodos.
  - Protección de puertos de diagnóstico remoto.
  - Control de enrutamiento en red.
  - Seguridad de los servicios de red.

2.2.1.8 DESARROLLO Y MANTENIMIENTO DE SISTEMAS.

No está garantizado que la seguridad está incorporada en los sistemas de información.

- **Seguridad de las aplicaciones del sistema.**
  - Validación de los datos de entrada.

- Control de procesamiento interno.
- Validación de los datos de salida.

- **Seguridad de los archivos del sistema.**
  - Control del software operativo.
  - Control de acceso a la librería de programas fuente.
- **Seguridad en los procesos de desarrollo y soporte.**
  - Procedimientos de control de cambio.
  - Revisión técnica de los cambios en el sistema.

2.2.1.9 GESTIÓN DE CONTINUIDAD DEL NEGOCIO.

Todas las situaciones que puedan provocar la interrupción de las actividades hospitalarias deben ser prevenidas y contrarrestadas mediante los planes de contingencia adecuados.

- **Aspectos de la gestión de la continuidad del servicio de salud.**

  Estructura para la planificación de la continuidad del servicio de salud.

  Se deben definir equipos de recuperación ante contingencias, en los que se identifiquen claramente las funciones y responsabilidades de cada miembro en caso de desastre.

2.2.1.10 CONFORMIDAD CON LA LEGISLACIÓN.

Se debe identificar convenientemente la legislación aplicablea los sistemas de información corporativos, integrándola en el sistema de seguridad de la información de la compañía y garantizando su cumplimiento.

- Cumplimiento con los requisitos legales.
- Revisiones de la política de seguridad y del cumplimiento técnico.
- Consideraciones de la auditoría de sistemas.

Se debe definir un plan de auditoría interna y ser ejecutado convenientemente, para garantizar la detección de desviaciones con respecto a la política de seguridad de la información.

2.2.2 SITUACIÓN ACTUAL DE HARDWARE.

El Hospital de Especialidades cuenta con la estructura de servidores:

- **Un BladeCenter H**, con 8 cuchillas de diferentes modelos y características. Los slots de las cuchillas están numerados desde el número 1 hasta el 14 de izquierda a derecha, como se indica en el gráfico 2.3.

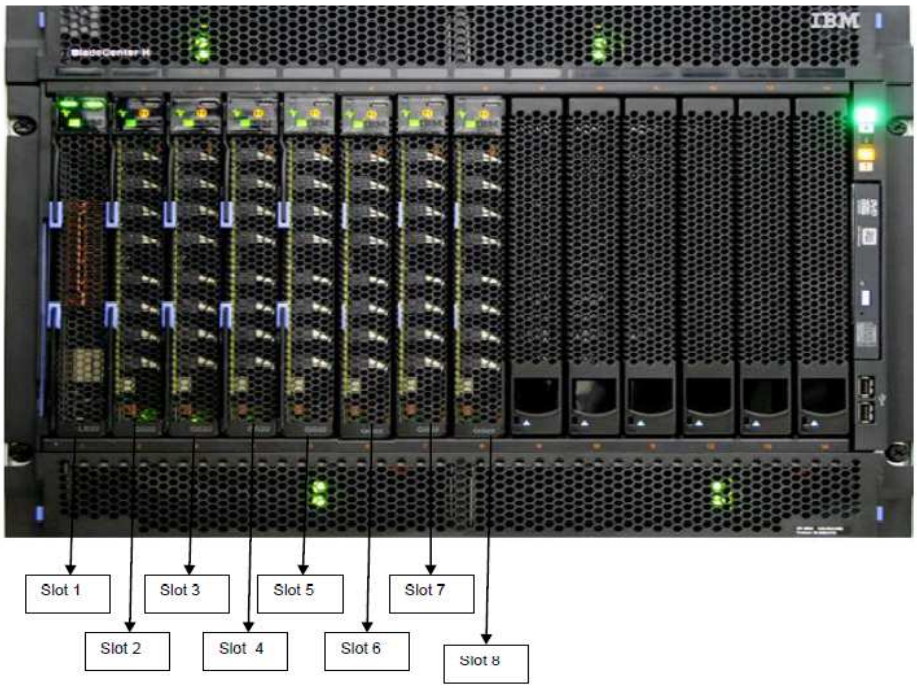


Gráfico 2.3: BladeCenter H

- **Cuchillas**

  Las cuchillas cuentan con las siguientes características indicadas en la Tabla 2.1

Tabla 2.1: Cuchillas instaladas en el BladeCenter

UBICACIÓN	HARDWARE	SIST OPERATIVO	RAM	DISCO INTERNO TOTAL	DISCO STORAGE
Slot 1	Hs21	ESXi 5.1 Administrado por vCenter 172.16.60.99	GB	**Datastore 1** Total 60 GB Libre: 58Gb	**Netapp**
Slot 2	Hs21	ESXi 5.1 Administrado por vCenter 172.16.60.99	GB	**Datastore 1** Total: 557GB Libre: 555GB	**Netapp**
Slot 3	Hs21	ESXi 5.1 Administrado por vCenter 172.16.60.99	GB	**Datastore 1(1)** Total: 131GB Libre: 130GB	**Netapp**
Slot 4	Hs21	ESXi 5.1 Administrado por vCenter 172.16.60.99	GB	**Datastore 1(1)** Total: 131GB Libre: 130GB	**Netapp**
Slot 5	Hs21	ESXi 5.1 Administrado por vCenter 172.16.60.99	GB	**Datastore 1(1)** Total: 131GB Libre: 130GB	**Netapp**
Slot 6	Hs21	ESXi 5.1 Administrado por vCenter 172.16.60.99	GB	**Datastore 1(1)** Total: 146GB Libre: 140GB	**Netapp**

Slot 7	Hs21	ESXi 5.1 Administrado por vCenter 172.16.60.99	GB	**Datastore 1(1)** Total: 50GB Libre: 40GB	**Netapp**
Slot 8	Hs21	ESXi 5.1 Administrado por vCenter 172.16.60.99	GB	**Datastore 1(1)** Total: 50GB Libre: 40GB	**Netapp**

- **Servidores tipo rack 3650 M3**

Tabla 2.2: Servidores 3650 M3,

NOMBRE	HARDWARE	SIST. OPERATIVO	RAM	DISCO INTERNO TOTAL
Servidor 1	X3650M3	ESXi 5.0	73 GB	**Datastore 1** Total: 131GB Libre: 130GB Data Storage 1TB Total: 930 GB Libre 327GB
Servidor 1	X3650M3	ESXi 5.0	73 GB	**Datastore 1** Total: 131GB Libre: 130GB Data Storage 1TB Total: 930 GB Libre 327GB

Gráfico 2.4: Storage DS4700

En este storage están configuradas 2 LUNs:

- DT_Particion1_600GB.
- Blade 3.4_Storage5.6_RAID1:

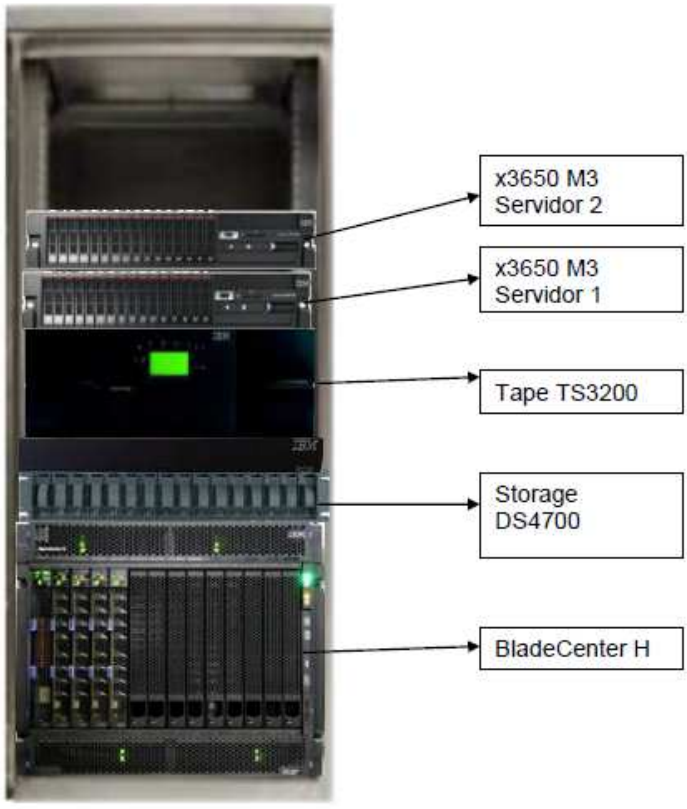


Gráfico 2.5: Diagrama Físico

- **Software**

  La infraestructura del HE-1 está basada en WMware, ya que todos los servidores y cuchillas tienen instalado un hipervisor, además de un vCenter que administra las cuchillas ubicadas en los slots 3,4 y 5.

  - El hardware de escritorio se basa en computadores de marca lenovo y ciertos clones, que deberán ser renovadas y actualizadas.
  - Los equipos de comunicaciones y redes se basan en tecnología 3 Com, Son insuficientes conforme a las necesidades del HE-1, y se requiere adquirir equipos tanto de comunicaciones como de seguridad de redes, para poder realizar una mejor administración.
  - La red de datos y comunicaciones del HE-1 es de tipo LAN distribuida entre los pisos de la entidad y basadas en topología estrella, en la que se encuentra migrado en un 60% a 1GB.
  - La red eléctrica computacional no abastece a todos los computadores instalados en el HE-1, su instalación a tierra es inadecuada, así como también sus protecciones de para rayos. No dispone el HE-1 de una red de energía estabilizada para la red de datos.

2.2.3 SITUACIÓN ACTUAL DEL SOFTWARE DEL HE-1.

- Los sistemas informáticos del HE-1, no forman parte de un sistema integrado, como es el caso de las áreas Financieras, Activos Fijos y Nómina.
- Los sistemas informáticos descentralizados tienen autonomía en la administración de los mismos.

- Las Áreas que utilizan sistemas informáticos descentralizados del Dpto. de Tecnologías de la Información y Comunicaciones son responsables de la custodia física de los servidores de aplicaciones y bases de datos.
- El HE-1 al tener operando en sus procesos de operación sistemas informáticos descentralizados insuficientes en cantidad y calidad obliga a que algunos procesos se lo realicen de forma manual.
- La falta de consolidación de datos computacionales relacionados, provoca que la información sea inoportuna e inexacta, afectando la administración, gestión y producción del HE-1.

2.2.3.1 Atención al cliente

En esta área existe un sistema informático que cubre de forma parcial las expectativas, se llama SISTEMA DE CAJAS está desarrollado en el lenguaje de programación Developer 2000 de ORACLE, almacena su información en la base del mismo nombre del HE-1 y está bajo la responsabilidad del área de Sistemas y Comunicaciones.

Diagnóstico

Esta área no posee un sistema informático integrado con las demás áreas del HE-1 que permita obtener resultados adecuados para el trabajo que realiza el área de Comercialización y Comunicación Social en el subproceso de Atención al Cliente.

2.2.3.2 Venta directa

Para este proceso existe en esta área un sistema informático que permite cubrir las necesidades y expectativas del área, éste se llama SISTEMA DE FACTURACIÓN Y CAJAS, está desarrollado en el lenguaje de programación Developer 2000 de ORACLE, su información se almacena en la base de datos del HE-1.

Diagnóstico

Este sistema informático debe integrarse con áreas como finanzas, y la parte asistencial del HE-1 de forma directa y en la actualidad esto no es así, por lo tanto se concluye que no posee un sistema informático integrado con todas las áreas que automatice los procesos para el trabajo que realiza el área de Comercialización y Comunicación Social en el subproceso de Venta Directa.

2.2.3.3 Convenios

No existe en el área de Comercialización y Comunicación Social para el subproceso de Convenios un sistema informático que permita llenar las expectativas y necesidades del área.

Para el desarrollo automatizado del trabajo, se utiliza software de oficina en PC.

Se utiliza herramientas de oficina Microsoft Word para informes y Excel para cuadros estadísticos, Power Point para presentaciones.

Diagnóstico

No posee un sistema informático integrado que automatice los procesos para el trabajo que realiza el área de Comercialización y Comunicación Social en el subproceso de Promociones y Comunicaciones.

2.2.3.4 Ingreso a emergencia

En el área existe un sistema informático que les permite automatizar su proceso de forma integrada con el módulo de facturación del HE-1.

El sistema informático denominado CAJAS que existe en el área de Ingreso a Emergencia está desarrollado con Developer 2000 de ORACLE.

Diagnóstico

- Actualmente el sistema informático existente en el HE-1 llamado CAJAS(sistema de facturación - observación), permite facturar en el área de Ingreso a Emergencia.
- Este sistema informático no se integra con todas las áreas del HE-1 haciendo que los procesos relacionados con éste sean manuales.

2.2.3.5 Apertura de historia clínica

Para la apertura de la historia clínica de pacientes existe un sistema informático que no llena con todos los requerimientos y necesidades de este proceso y del área en sí de Emergencia.

Se denomina SISTEMA DE FACTURACIÓN - CAJAS se encuentra desarrollado con Developer 2000 de ORACLE. En el sistema informático que utiliza el área de Emergencia, se puede consultar e ingresar los datos del paciente de la ficha médica, pero algunos procesos se los realiza manualmente.

Diagnóstico

No posee un sistema informático integrado que automatice los procesos para el trabajo

que realiza el área de Emergencia en el subproceso de la Apertura de la Historia Clínica.

2.2.3.6 Atención en emergencia

No existe un sistema informático que les permite automatizar el desarrollo de sus procesos, para el desarrollo automatizado del trabajo, se utiliza software de oficina en PC, herramientas de oficina Microsoft como Word para informes y Excel para realizar formatos de ayuda para la Atención en Emergencia.

Diagnóstico

No posee un sistema informático integrado con todas las áreas que automatice los procesos para el trabajo que realiza el área de Emergencia en el subproceso de Atención en Emergencia.

2.2.3.7 Área de críticos

No existe un sistema informático que automatice los procesos relacionados con la gestión del trabajo del área.

Diagnóstico

No posee un sistema informático integrado con todas las áreas que automatice los procesos para el trabajo que realiza el área de Emergencia en el subproceso de Área de Críticos.

2.2.3.8 Observación

Existe un sistema informático que no cubre todas las necesidades y expectativas del área, se llama SISTEMA DE FACTURACIÓN - OBSERVACIÓN que solamente permite la facturación de este proceso. Se encuentra desarrollado en el lenguaje de

programación Developer 2000 de ORACLE.

Diagnóstico

El sistema informático que automatiza este proceso, permite realizar un trabajo local al no poder relacionarse con los sistemas informáticos del resto de áreas del HG-1.

2.2.3.9 Procesos de secretaria

No existe en el área un sistema informático que permita llenar las expectativas y necesidades del área.

Diagnóstico

No posee un sistema informático integrado que automatice los procesos para el trabajo que realiza el área de Emergencia de los Procesos de Secretaria.

2.2.3.10 Concesión de turnos

Para la automatización de este proceso, existe un sistema informático denominado SISTEMA DE FACTURACIÓN – AGENDA MÉDICA que se encuentra implantado en el área de Consulta Externa; esta desarrollado con Developer 2000 de ORACLE.

Se lo utiliza para realizar la apertura de la ficha del paciente, pero muchos de sus procesos se los realiza de forma manual.

Diagnóstico

- Este sistema informático permite automatizar los procesos de esta área de forma parcial ya que no se integra y relaciona con las demás áreas del HE-1.
- El sistema informático a implantarse debe permitir la obtención de cuadros estadísticos de las emergencias realizadas, agenda médica, número de pacientes

atendidos, cantidad de exámenes realizados.

- Que el sistema informático a implantarse debe permitir el ingreso de información con facilidad y emitir información actualizada de las áreas de: (Consulta Externa, y Emergencia).

2.2.3.11 Pedido de exámenes

En el área auxiliar diagnóstico y tratamiento se encuentra implantado un sistema informático que no permite automatizar en su totalidad los de los Pedidos de Exámenes.

El sistema informático instalado se denominado SISTEMA DE FACTURACIÓN – CAJAS que también existen en el área de Pedido de Exámenes, se encuentra desarrollado con Developer 2000 de ORACLE.

2.2.3.12 Farmacia

En el área de Farmacia existe un sistema informático denominado SISTEMA DE FACTURACIÓN – CAJAS y ABASTECIMIENTOS desarrollado con Developer 2000 de ORACLE. El sistema informático que utiliza el área de Farmacia, se lo utiliza para ingresar el pedido de medicamentos y su seguimiento y reportes de los insumos médicos existentes. Este sistema no automatiza en su totalidad los procesos del Área de Farmacia del HE-1.

2.2.3.13 Banco de sangre

El sistema informático denominado COMPULAB desarrollado en Visual Basic y FOXPRO, procesa y almacena en un mismo computador los resultados de los Exámenes de Sangre del HE-1.

Diagnóstico

- Es necesario implantar un sistema informático que permita reemplazar a este sistema y que permita relacionarse con los sistemas informáticos de todas las áreas del HE-1.
- Es necesario que el sistema informático a implantarse permita obtener reportes de exámenes de sangre más detallados como su almacenamiento por tipo de sangre, etc.
- El sistema informático a implantarse debe permitir el ingreso de información con facilidad y emitir información actualizada del Banco de Sangre del HE-1.

C A P Í T U L O III:

DEFINICIÓN E IMPLEMENTACIÓN DE UNA RED SEGURA.

3.1 GESTIÓN DE RIESGOS E IMPLEMENTACIÓN DE CONTROLES

3.1.1 GENERALIDADES

Proceso: Gestión de riesgos.

Frecuencia de ejecución: Bajo demanda

3.1.2 OBJETIVOS

- Identificar y minimizar la probabilidad de materialización de los riesgos que afecten a los procesos críticos de la Institución, soportados por la red LAN.
- Identificar y minimizar la probabilidad de materialización de riesgos que puedan afectar a los proyectos críticos.

3.1.3 NIVELES DE RESPONSABILIDAD

Responsable	Funciones de responsabilidad
Comité de seguridad	• Aprobar esta política y otorgar lineamientos y criterios generales para la gestión de riesgos. • Aprobar acciones y planes de mitigación de riesgos críticos que puedan afectar a la red de datos del HE-1.
Jefe de tecnología	• Revisar periódicamente los riesgos que puedan afectar a la red de datos. • Gestionar y dar seguimiento a la implementación de controles para mitigar los riesgos que puedan afectar a la red de datos del HE-1. • Definir los plazos de mitigación de cada riesgo y un responsable.
Directores de Departamento	• Ejecutar los planes de acción para mitigar los riesgos identificados

3.1.4 DESCRIPCIÓN DE LA POLÍTICA (Normas y disposiciones generales)

- Es obligación de todos los miembros del Departamento de Desarrollo Tecnológico y deproyectoscríticos informaral Oficial de Seguridadla

existencia de debilidades oamenazas quepuedanafectaralosintereses o procesos de la Red LAN.

- El Oficial de Seguridadtienelaobligacióndedetectarysugerircontrolesparamitigarlosriesgosidentificadosbasándoseenunplandeacciónaprobadoporel Departamento de Desarrollo Tecnológico.
- Dependiendo del nivel de riesgo se establecerá niveles de escalamiento para la solución de los problemasqueafectenala Red LAN.
- En casodeexistirriesgoscríticosoqueafectensignificativamenteala Red LAN del HE-1, el plan deacciónde beaprobarloelComitédeSeguridad definido.
- LosriesgoscríticosqueseráninformadosalComitédeSeguridaddeben presentar indicadores como costo, valor y retorno de inversión,conlafinalidaddefacilitaralosnivelesdirectivoslatomadedecisiones.
- EnelAnexoAsedetallanlasescalasde:Probabilidaddeocurrenciade RiesgoeImpactoencasodematerialización del riesgo.
- No se definirácuantitativamente el apetito de riesgo en términos económicos. Loslímitesde apetitoderiesgodependerándecada proyectoydeberánsermitigadostodosaquellosriesgosqueafectena laoperaciónInstitucionaly/oalcumplimientodelosobjetivosprincipalesdeunproyecto.

- Cualquierlineamientogeneralocambioenlapriorizacióndemitigaciónderiesgod ebeseraprobadaporelComitédeSeguridad.

Tabla 3.1: Escalas de impacto de riesgo sobre el HE-1

IMPACTO	MUY BAJO	BAJO	MEDIO	ALTO	MUY ALTO
Cualitativo	Pérdida o daño insignificante. No aumenta las quejas de los usuarios. No hay impacto	Pérdida o daño menor. Aumentan las quejas de los usuarios. Impacto mínimo	Pérdida significativa. Reclamos de usuarios a gran escala.	Pérdida o daño mayor. Investigación formal del regulador y aplicación de multas.	Pérdida catastrófica. Riesgo inaceptable en el sector. Intervención de ente regulador.
Objetivos	Impacto insignificante en el logro de los objetivos.	Impacto menor que es fácilmente remediable.	Algunos objetivos son afectados	Algunos objetivos importantes no pueden ser alcanzados.	La mayoría de los objetivos no pueden ser alcanzados.
Reputación e imagen	El evento solo es de conocimiento de los directamente involucrados	El evento es de conocimiento general de la organización	El evento es de conocimiento a nivel local	El evento es de conocimiento a nivel nacional	El evento es de conocimiento a nivel internacional

Legal	Los activos no se ven expuestos a pérdidas ni comprometidos por vulnerabilidad de ámbito legal alguna. Las operaciones no se ven afectadas. Los pasivos y contingentes se incrementan en un nivel insignificante. Quejas de Usuario	Los activos se ven expuestos a pérdida y comprometidos en un nivel menor debido a la explotación de alguna vulnerabilidad en el ámbito legal. Las operaciones se ven afectadas en un nivel menor. Los pasivos y contingentes se incrementan en un nivel no importante. Quejas y Posible Establecimiento de Demanda	Los activos se ven expuestos a pérdida y comprometidos en un nivel moderado debido a algunas vulnerabilidades de ámbito legal. Las operaciones se ven afectadas de manera negativa en un nivel considerable. Los pasivos y contingentes se incrementan en un nivel importante. Demanda Propuesta con Pérdidas Económicas	Los activos se ven expuestos a pérdida y comprometidos en un nivel grave debido a la exposición de varias vulnerabilidades de ámbito legal. Las operaciones se ven afectadas negativamente en un nivel grave. Los pasivos y contingentes se incrementan de manera grave. Demanda con Pérdidas Económicas e Intervención de Entes Reguladores	Los activos se ven expuestos a pérdida y comprometidos en un nivel crítico debido a la explotación de varias vulnerabilidades de ámbito legal. Las operaciones de la organización fueron suspendidas. Los pasivos y contingentes se incrementan en un nivel crítico. Demanda Procede con pérdida. Ente Regulador

Tabla 3.2: Niveles de escalamiento.

Nivel de Impacto	A nivel de Área de Incidente	A nivel de HE-1	A nivel Gobierno	A nivel Externo
Muy Bajo	Reporte al Supervisor	No	No	No
Bajo	Reporte al Supervisor	lotificación a Dirección	No	No
Medio	Reporte al Supervisor	Reporte a Presidencia	cación a Organismo de Control	No
Alto	Reporte al Supervisor	Reporte a Presidencia	eporte a Organismo de Control	Notificación Pública
Muy Alto	Reporte al Supervisor	Reporte a Presidencia	eporte a Organismo de Control	Reporte Público

* Notificación incluye el poner el conocimiento

** Reporte implica una descripción detallada de los hechos

*** Los reportes públicos debe intervenir Departamento de Comunicación.

A nivel de cada área ante la presencia de un incidente, el funcionario responsable tiene la obligación de emitir un reporte hacia el Director del Área de Trabajo, a su vez si el problema se encuentra relacionado con otras áreas, el Director o jefe, es el encargado de emitir un reporte a los Directores de Áreas involucradas en el Incidente.

Si el problema se encuentra en un nivel medio de impacto el Director de Área tiene la obligación de generar un reporte del incidente hacia el Director del Hospital.

En caso de que el nivel de incidencia sea alto o muy alto es de responsabilidad de la Dirección General la generación de un reporte hacia los organismos de control y el manejo al exterior que se deba dar al incidente con la respectiva aprobación de los diferentes organismos del estado Ecuatoriano.

Tabla 3.3: Solución

Nivel de Impacto	A nivel de Área de Incidente	A nivel de HE-1
Muy Bajo	**Solución a nivel de Área**	
Bajo	**Solución a nivel de Área**	
Medio		**Solución a nivel de HE-1**

Si bien la solución está establecida de acuerdo al área responsable, los reportes y notificaciones deben ser presentados de acuerdo a lo establecido.

3.1.5 CÁLCULO DEL NIVEL DE RIESGO

Qué puede ir mal?

- Que la red LAN implementada no funcione.

- Que los equipos activos de red como son: los switches de piso y de core, los servidores, la base de datos no funcionen.
- Que la red eléctrica no abastezca o no tenga una red de energía estabilizada para la red informática donde corre el sistema de gestión hospitalario.

Con qué frecuencia puede ocurrir?

No existen estadísticas ni registros y podría ocurrir en cualquier momento

Cuál sería sus consecuencias?

Se suspendería la gestión hospitalaria en los servicios de salud, como atención médica en emergencia, cuidados intensivos, hospitalización, consulta externa.

Lo que sería extremadamente peligroso por cuanto más del 90% de los procesos médicos se encuentran automatizados y atentaría incluso con la atención de los pacientes.

Tabla 3.4: Tipo de Riesgos

Tipo de riesgo	Factor
Robo de hardware	Alto
Robo de información	Alto
Falla en los equipos activos de red	Medio
Virus informático	Medio
Equivocaciones	Medio
Accesos no autorizados	Medio

Niveles de riesgos

Como puede apreciarse en la tabla anterior, los riesgos se clasifican por su nivel de importancia y por la severidad de su pérdida:

- Estimación del riesgo de pérdida del recurso Ri.
- Estimación de la importancia del recurso Ii.

Para cuantificar el riesgo de perder un recurso, se asigna un valor numérico del 1 al 10, tanto a la importancia del recurso (10 es el recurso de mayor importancia) como al riesgo de perderlo (10 es el riesgo más alto).

El riesgo de un recurso es el producto de su importancia por el riesgo de perderlo mediante la fórmula (1) $WRi = Ri * Ii$ **(1)**

Con la fórmula**(2)** es posible calcular el riesgo general de los recursos de la red:

$$WR = \frac{(WR1*I1+WR2*I2+\ldots+WRn*In)}{I1+I2+I\ldots In} \quad \textbf{(2)}$$

Para obtener una red segura se ha estimado los siguientes riesgos y su importancia para los elementos de la red que se administra como se indica en la tabla 3.6

Tabla 3.6: Evaluación de riesgos.

Recurso	Riesgo (Ri)	Importancia (Ii)	Riesgo evaluado(Ri*Ii)
Switch de core	6	7	42
Switch de borde	6	5	30
Servidores	10	10	100
PC´s	9	2	18
Base de datos	10	10	100

Aquí ya se puede apreciar que el recurso que más debe protegerse es el servidor.

Parala obtención del riesgo total de la red calculamos mediante la fórmula (3):

$$WR = \frac{42+30+100+18+100}{7+5+10+2+10} = 8{,}52 \textbf{(3)}$$

Al ver que el riesgo total de la red es casi 8,52 puntos sobre 10 deberían pensarse seriamente en buscar las probables causas que pueden provocar problemas a los servicios brindados por los elementos evaluados.

Identificación de amenaza

Una vez conocido los riesgos, los recursos que se deben proteger y como su daño o falta pueden influir en esta casa de salud es necesario identificar cada una de las amenazas y vulnerabilidades que pueden causar estas bajas en los recursos. Existe una relación directa entre amenaza y vulnerabilidad a tal punto que si una no existe la otra tampoco.

Las amenazas existentes según su ámbito de acción son:

- Amenazas del sistema (Seguridad lógica y física).
- Amenazas en la red (Comunicaciones).

Evaluación de costos

Establecer el valor de los datos es algo totalmente relativo, pues la información constituye un recurso que, en muchos casos, no se valora adecuadamente debido a su intangibilidad, cosa que no ocurre con los equipos, la documentación o las aplicaciones.

Qué recursos se quieren proteger?

Hardware: PC´s, Switches de distribución, Switches de core, los servidores y la base de datos.

De qué se quiere proteger estos recursos?

De errores humanos, desconfiguraciones, circuitos eléctricos.

Qué tan reales son las amenazas?

Se pueden dar por falta de conocimiento o errores involuntarios, inestabilidad de la red eléctrica.

Qué tan importante son estos recursos?

Altamente importantes, por cuanto sobre esta infraestructura de red se encuentra la aplicación informática del sistema de gestión hospitalario.

Por tanto los recursos citado anteriormente vale la pena proteger ya que tienen un alto costo como se indica en la tabla 3.7:

Tabla 3.7: Recursos empleados en el HE-1 para la infraestructura tecnológica

Ord	PROYECTO	COSTO
1	Implementación Data Center	110.000
2	Implementación de Cableado Estructurado	87.100
3	Adquisición de equipamiento informático	177867
4	Implementación de una red de energía estabilizada	220.000
5	Adquisición para infraestructura de redes	433185
	TOTAL	1.028.152

A este costo se puede añadir la pérdida por la interrupción del sistema de gestión hospitalario lo que se incrementaría sustancialmente y más aún en poner en juego la vida de los pacientes en esta casa de salud por la no disposición de la red de datos en mantenerse disponible en un 100%.

De acuerdo a los pilares de la seguridad ISO 17799 y el análisis de riesgos, enfocaremos a los dominios de control que se relacionan directamente con:

La seguridad lógica:

- Control de accesos.
- Desarrollo y mantenimiento de sistemas.
- Gestión de comunicaciones y operaciones.

La seguridad Física:

- Seguridad física y del entorno.

3.2 POLÍTICA DE SEGURIDAD PARA UNA RED SEGURA:

Hoy es imposible de hablar de un sistema cien por cien seguros, sencillamente porque el costo de la seguridad total es muy alto. Por eso las empresas, en general, asumen riesgos.

Las Políticas de Seguridad para una red segura surgen como una herramienta organizacional para concientizar a cada uno de los miembros de esta casa de salud sobre la importancia y sensibilidad de la información que circula por la red hospitalaria.

Objetivo de control: Bridar orientación y apoyo de la dirección para la seguridad de la red.

3.2.1 Definición de la seguridad de la red.

La seguridad de la red informática hospitalaria es un activo importante del servicio de salud, tiene valor para el Hospital de Especialidades de FFAA, y requiere en consecuencia, una protección adecuada. La seguridad de la red protege a esta, de una amplia gama de amenazas, para asegurar la conectividad de la red y la continuidad del servicio de salud y administrativo.

La seguridad de la red se caracteriza por disponer de su funcionamiento continuo y permanente las 24 horas del día, los 7 días de la semana, los 365 días del año, a fin de que brinde el apoyo eficiente a los procesos sustantivos del hospital como son:

A. Evaluación médica.
B. Tratamiento médico.
C. Rehabilitación médica.
D. Atención paliativa.

Basados en los procesos adjetivos de apoyo y asesoría, con el objetivo general de proporcionar atención médica integral de tercer nivel con calidad y calidez; al personal militar en apoyo a las operaciones militares y con su capacidad disponible al personal militar en servicio pasivo, dependientes, derechohabiente y a la población civil, dentro del sistema de referencia y contra-referencia militar y nacional".

3.2.2 Alcance de la seguridad de la red

El alcance de la seguridad de red está orientado básicamente a:

- Privacidad e Integridad.
- Disponibilidad y Autenticidad.
- De la red LAN del Hospital de Especialidades de FFAA.

3.2.3 Importancia de la seguridad de la red:

La seguridad de la red informática, ha adquirido una gran importancia en los tiempos más recientes, sobre todo para las organizaciones como hospitales. Esta situación se debe a que día a día las amenazas informáticas, como lo son los intrusos o programas maliciosos, representan un problema serio que merece tener una atención especial, ya que podrían tener grandes efectos si se afecta la conectividad de la red, o accedieran a información confidencial pudiendo usarla de manera no apropiada.

Además, la seguridad de la red informática en el ámbito de salud, también es de gran importancia hacer respaldos de la información y tenerla disponible sin correr el riesgo de perderla, por lo que se requiere disponer de la historia clínica, pacientes sub subsecuentes, turnos, programación de exámenes, etc.

De igual forma, es vital mantener en óptimo funcionamiento a todos los equipos activos de red, que formen parte de la red del sistema de gestión hospitalario, teniendo la capacidad de evitar pérdidas o robos de la información u otros problemas que afecten a la infraestructura informática y al servicio de salud.

Otra parte importante son los usuarios que tendrán acceso a los equipos computacionales, por ello el departamento responsable de la seguridad de la red informática deberá de hacer ciertas restricciones en los perfiles y limitar la accesibilidad a determinados sitios con el fin de asegurar un estado óptimo en las equipos; aparte de dar cierta capacitación a los usuarios antes mencionados.

3.2.4 Disposiciones generales

- Asegurar a un nivel razonable que todos los medios de procesamiento y/o conservación de información cuenten con medidas de protección física y lógica que eviten el acceso y/o utilización indebida por personal no autorizado, así como permitan la continuidad de las operaciones. Esto incluye repositorios de archivos de manejo de propiedad intelectual y la gestión de activos informáticos para que estos reciban un apropiado nivel de protección y respaldo.
- El funcionamiento correcto y seguro de los equipos activos de red incluye respaldos, configuraciones que serán establecidos por el administrador de red. De esta manera la información estará disponible en el momento necesario únicamente para los usuarios autorizados. Considerando la continuidad de la operación tecnológica que soporta los procesos institucionales.
- Asegurar que los datos y/o transacciones cumplan con los niveles de autorización

correspondiente para su utilización y divulgación.

- Permitir el registro e identificación inequívoca de los usuarios en los diferentes sistemas informáticos, usar identificadores únicos.
- Evitar casos de suplantación de identidad por medio de los recursos tecnológicos.
- Mantener registros de auditoría de los eventos ocurridos así como el responsable de su ejecución.
- La identificación y análisis de riesgos relacionados al ambiente tecnológico que permitan disponer de una arquitectura operacionalmente segura.
- El Departamento de Tecnologías de la Información y Comunicaciones es el responsable de acreditar las áreas de Desarrollo, Administración de Bases de Datos, Hardware, Redes, Comunicaciones, Mantenimiento y Software en general de la institución, autorizadas por normativa, para el desarrollo e implementación de proyectos en tecnologías de información, considerando los recursos disponibles y el cumplimiento de la normativa y los estándares institucionales.
- Los equipos activos de red deben ser de la misma tecnología a los instalados, de manera de estandarizar la infra estructura de red.
- Para la implementación de puntos de red se deberá utilizar las especificaciones técnicas que suministre el Departamento de Tecnologías de la Información, diseñada con base en las normas establecidas para cableado estructurado.
- El Departamento de Tecnologías de la Información y Comunicaciones es la unidad responsable de la definición, administración de la red.
- El Departamento de Tecnologías de la Información y Comunicaciones es la unidad técnica responsable de evaluar las ofertas para la adquisición del hardware, software

y servicios informáticos que se requieran para la operación de sistemas de ámbito institucional.

- Los servicios de información del World Wide Web son competencia del Área de Sistemas y Comunicaciones y las diferentes unidades departamentales de trabajo de la Institución, deben suscribir el servicio con esta instancia.
- Para aceptar donaciones de hardware, software, comunicaciones y cualquier tipo de tecnologías de información, éstas deben cumplir con los estándares, la plataforma técnica, las políticas y la normativa vigente, y cuenten con la recomendación técnica del Área de Sistemas y Comunicaciones.
- Las diferentes unidades departamentales de trabajo de la Institución deben responder ante la Auditoria de Informática por el incumplimiento de lo establecido en los manuales técnicos, operativos y organizacionales que rigen el desarrollo del área informática institucional.
- Los diferentes sistemas de información en todos los niveles de la organización, deben contar con los mecanismos de seguridad para prevenir la implantación de sistemas de información con riesgos considerables.

3.2.5 Organización administración y mantenimiento de la red.

La organización, administración y mantenimiento de la red es responsabilidad del Departamento de tecnología de la información del HE-1. Para lo cual deben coordinar con el Área de administración de red, Desarrollo, HelpDesk y documentar los desarrollos de nuevo hardware, mantenimientos preventivos, correctivos así como las

configuraciones de red de todos los equipos activos de red como son: switches, Firewall, IPS, disponer de bitácoras , diagramas de red, etc.

3.2.6 Seguridad de la gestión

- Se deben elaborar, actualizar y aprobar en los niveles correspondientes, los Planes de Contingencia en las unidades departamentales de trabajo que utilicen para su funcionamiento sistemas de red, para asegurar la operación normal de la misma cuando se presenten eventualidades inesperadas que afecten su funcionamiento, estos planes deben estar documentados, aprobados por la autoridad correspondiente y puestos a prueba.
- Las diferentes unidades departamentales, servicios médicos que operan con el sistema de gestión hospitalaria, deben mantener respaldos y actualizaciones de los archivos de datos, de los programas, con el propósito de asegurar la prestación de los servicios a los usuarios internos y externos.
- Los respaldos de archivos institucionales, estratégicos y críticos deben mantenerse en un lugar externo al centro de procesamiento, el acceso de personas a estas áreas será restringido y controlado.
- El data center debe contar con dispositivos de seguridad para el acceso a fin de garantizar que únicamente los funcionarios autorizados, tengan acceso al área.

3.2.7 Políticas informáticas especiales.

Las políticas informáticas especiales se definen como complemento y en algunos casos detallan las políticas institucionales actuales en el área informática.

Contratar consultores externos a fin de afinar, optimizar y garantizar una estabilidad permanente de la red de datos para el Hospital, y bajo la asesoría de las unidades departamentales respectivas en cumplimiento de la normativa institucional vigente, la Ley de Contratación Pública y sus Reglamentos.

3.2.8 Revisión y evaluación

La Dirección General del HE-1 ha definido un documento con una política clara, existe una definición de la seguridad de la red y sus objetivos globales, el alcance de la seguridad y su importancia, así como políticas de seguridad, principios, normas y requisitos de cumplimiento, definición de responsabilidades generales y especificas en materia de gestión de la seguridad de la red.

Esta política debe ser revisada y evaluada de manera continua por parte del planificador informático del HE-1 y Jefe del departamento de sistemas, a fin de poder incorporar en esta metodología el proceso de mejora continua.

3.3 SEGURIDAD ORGANIZACIONAL

3.3.1 Estructura para la seguridad de la red.

El objetivo de este control es gestionar la seguridad de la red dentro del HE-1.

3.3.1.1 Comité de la dirección sobre la seguridad de la red

La seguridad de la red es una responsabilidad compartida con todos los miembros de esta casa de salud, por lo cual se define un comité de seguridad de la Información que integra miembros de la alta dirección para el apoyo de las iniciativas de seguridad de la información.

El comité estará conformado por:

- Director General del Hospital (o su delegado).
- Jefe del Departamento de Tecnologías de la Información y Comunicaciones.
- Planificador del Departamento de Tecnologías de la Información y Comunicaciones.
- Administradores de red y base de datos.

Este comité tendrá la responsabilidad de revisar y aprobar la Política de seguridad de la red, así como también supervisará el Plan de Seguridad de la red de manera ejecutiva mediante:

- Revisión y aprobación de la política de la seguridad de la red y de las responsabilidades principales.
- Supervisión y control de los cambios significativos en la estructura, configuración, administración y mantenimiento de la infraestructura de la red.
- Revisión y seguimiento de los incidentes de la red.
- La definición de proyectos de tecnologías que fortalezcan la seguridad de la red.

Responsabilidades del Comité de Seguridad de la red

Este comité tendrá la responsabilidad de revisar y aprobar la Política de Seguridad de la red, así como también; supervisará el Plan de Seguridad de la red de manera ejecutiva mediante:

- La revisión anual del Plan Estratégico del Área Seguridad
- La definición de proyectos de tecnologías que fortalezcan la Seguridad de la

Información (Servicio, Producto e Información).

- Aprobar el Manual de Gestión de Seguridad de la Información y el plan de difusión respectivo, para lograr el compromiso de todos los usuarios de velar por el cumplimiento de todo el personal en cuanto a la política de Seguridad de la información establecida e informar al comité de Seguridad de la Información para las debidas acciones de acuerdo al proceso de control de cumplimiento para las respectivas acciones correctivas o preventivas.

Definición del Dueño de Datos de la red

Son todos los responsables de cada uno de los procesos y sistemas de información hospitalarios.

El Departamento de Desarrollo Tecnológico junto al Departamento de Desarrollo Institucional son los responsables de identificar los dueños de datos y hacer conocer a los mismos sus responsabilidades. En esta identificación se debe determinar también:

- Información
- Dueño de Datos
- Recursos informáticos que procesan la información
- Proceso Involucrado con la información

De manera general los dueños de datos son los Directores responsables de cada Departamento o Área al interior del HE-1.

Responsabilidades del Dueño de Datos de la red

- Deberá identificar toda la información confidencial que corresponda a su área de

responsabilidad directa cualquiera sea su forma y medio de conservación, para proceder a clasificarla de acuerdo a lo establecido en la Política de Gestión de activos.

- Deberá autorizar el acceso a su información a toda persona o grupo que requiera. Este acceso contemplará los privilegios respectivos (lectura, escritura, actualización y eliminación). Estos accesos estarán sobre sistemas informáticos y recursos organizacionales.
- Podrá delegar su función a personal idóneo, pero conservaran la responsabilidad del cumplimiento de la misma. Además, deberán verificar la correcta ejecución de las tareas asignadas. La delegación de funciones debe quedar documentado por el propietarios e informadas al Oficial de Seguridad de dicha delegación.
- Todo tratamiento sobre la información de la red que es responsabilidad del Dueño de Datos deberá recibir su aprobación, por lo que no se podrán tomar decisiones sobre dicha información que no sean puestas en su debido conocimiento y aprobadas por escrito hacia el Oficial de Seguridad y Jefe del DTIC del HE-1

Definición del Oficial de Seguridad de la red

El oficial de seguridad de la red tiene a su cargo la definición y el mantenimiento del Manual de Gestión de Seguridad de la red y el asesoramiento a todo el personal del hospital para su implementación.

Responsabilidades del Oficial de Seguridad de la red

- Deberá implementar un plan para concientizar a la administración acerca de la

importancia de dar seguridad según la criticidad de la información manejada en cada servicio a través de la red de datos.

- Deberá llevar a cabo el mantenimiento, aprobación, actualización, distribución y monitoreo del Manual de Gestión de Seguridad de la red en base a los requerimientos futuros presentados por nuevos servicios.
- Deberá proponer los proyectos de seguridad de la red para lo cual:
  - Deberá dar soporte a los usuarios y administradores en los procesos de:
  - Identificación de la información sensible.
  - Identificación de las medidas de seguridad necesarias en cada sistema para cumplir con el Manual de Gestión de Seguridad de la red.
  - Implementar dichas medidas.
- Deberá analizar e informar cualquier evento que atente contra la seguridad de la red al Jefe de Desarrollo Tecnológico, así como monitorear periódicamente que solamente los usuarios autorizados tengan accesos a la red de datos.
- Deberá someter al plan de seguridad de la red en una mejora continua.

DefinicióndelosAdministradoresdelosServicios de red

Se considera a las personas encargadas de llevar la administración de las aplicaciones, servidores, bases de datos y equipos de trabajo.

ResponsabilidadesdelosAdministradoresdelosServicios de red

- Deberán implementar las medidas de seguridad a fin de garantizar la seguridad de su servicio, en base a las recomendaciones del Oficial de Seguridad.

- Deberán apoyar a los proyectos que se planteen en torno al tema de seguridad de la red.
- Deberán controlar la correcta aplicación y control de accesos autorizados a los diferentes sistemas a su cargo. El control de accesos y permisos sobre aplicaciones y sistemas será entregado por el Oficial de Seguridad una vez que este ha evaluado que no compromete la seguridad de la información hospitalaria.
- El control de accesos y permisos será llevado a través de un documento de control de los mismos con las respectivas firmas de autorización.
- Deberán notificar al administrador de seguridad y al Jefe de Desarrollo Tecnológico de amenazas de seguridad presentes en la arquitectura de TI del hospital.

Definición de Usuario final

Se considera a todo el personal del hospital, de manera directa o indirecta y/o terceros que hacen uso de las aplicaciones y la información con el objetivo de poder cumplir con sus correspondientes funciones.

ResponsabilidadesdelUsuarioFinal

- Deberá cumplir con todas las medidas de seguridad definidas en el Manual de Gestión de Seguridad de la red.
- Deberá informar oportunamente cualquier amenaza o riesgo en el que los sistemas informáticos que maneja puedan ser expuestos o vulnerados.

- Deberá participar activamente de las capacitaciones periódicas para conocer de las medidas en el campo de Seguridad de la red a nivel del HE-1.

AutorizaciónparaInstalacionesdeProcesamientodeInformación

- La inclusión de nuevos usuarios al Sistema de Gestión Hospitalario.
- La inclusión de nuevos servicios para el procesamiento de la información deberá ser autorizada por el supervisor directo del funcionario, quien a su vez lo solicitará al dueño de datos involucrado y será entregada al jefe del Departamento de Tecnología y el Oficial de Seguridad para su aprobación y ejecución.
- El oficial de Seguridad en conjunto con el Departamento de Desarrollo Tecnológico implementará los accesos solicitados para el funcionario teniendo como respaldo el documento de autorización de accesos.
- El oficial de Seguridad en conjunto con el Departamento de Desarrollo Tecnológico deberá identificar e implementar controles de seguridad necesarios contra posibles vulnerabilidades introducidos por la implementación de nuevos sistemas que procese información.

Acuerdosdeconfidencialidad

- Todos los administradores de servicios deberán firmar un Acuerdo de Confidencialidad.
- Todo el personal que trabaja en el hospital deberá obligatoriamente firmar un Acuerdo de Confidencialidad, estos incluyen personal de planta, becarios de investigación, pasantes, personal externo.

Revisiónindependientedelaseguridaddelared

Se debe realizar revisiones independientes sobre la vigencia e implementación de la Política de Seguridad de la red, con el fin de verificar y garantizar que las prácticas de los diferentes procesos hospitalarios reflejen adecuadamente sus disposiciones.

3.3.1.2 Coordinación de la seguridad de la red.

Coordinar la implementación de los controles de la seguridad de la red:

- Establecer las funciones y responsabilidad específicas de la seguridad de la red en todo el HE-1.
  - Monitoreo de la red.
  - Actualización de software de red.
  - Configuraciones de red.

3.3.1.3 Asignación de responsabilidades para la seguridad de la red

La seguridad de la red está a responsabilidad del administrador de red del HE-1, quien debe seguir como guía la política de la seguridad de la red establecida.

Organizar, administrar y mantener la infraestructura de red comprendida por el sistema de cableado estructurado, los equipos activos de red (switches de piso, switch decore, firewall, IPS, entre otros).

Establecer claramente los niveles de acceso a los equipos activos de red.

3.3.1.4 Procesos de instalación para infraestructura de red.

- Los nuevos puntos de cableado estructurado no deben ser de categoría menor a la instalada en el HE-1 (categoría 6A) , previa la autorización del jefe de sistemas del HE-1.
- Los equipos activos de red deben cumplir con la estandarización, capacidad y configuraciones correspondientes, a fin de que sean compatibles con los demás componentes de la infraestructura de red.

3.3.1.5 Asesoría de un especialista en seguridad de redes.

Se debe tener acceso a asesores externos adecuados que aporten en todos los aspectos de la seguridad de la red.

3.3.2 Seguridad del acceso a la red de terceras personas.

El objetivo de este control es mantener la seguridad de la infraestructura de la red del acceso de terceras personas.

3.3.2.1 Tipos de acceso

Acceso lógico a los equipos activos de red: PCs, Swicth, Firewall, IPS, Base de datos.

3.3.2.2 Motivos de acceso

Existen terceras personas que pueden tener acceso lógico a los equipos activos de red porque dan servicios de soporte al HE-1, es de gran valor el acceso a la información sobre todo de la base de datos, para lo cual se debe tener un contrato perfectamente elaborado donde se estipula la confidencialidad de la información, la responsabilidad

que adquieren dicha empresa siendo responsables pecuniaria y penalmente del mal manejo de la información a la que tiene acceso.

Deben estar en contacto permanente con los administradores de la base de datos y de la red del HE-1.

3.4 CLASIFICACIÓN Y CONTROL DE ACTIVOS DE LA RED

3.4.1 Responsabilidad sobre los activos.

Objetivo de Control: Mantener la protección adecuada de los activos de la red de datos hospitalaria.

3.4.1.1 Inventario de activos físicos

- Elaborar, organizar y actualizar los inventarios de equipamiento informático (computadores de escritorio y portátiles).
- Elaborar, organizar y actualizar los inventarios de equipos activos de red (switches, servidores, firewall, IPS, etc.)
- Sistema de Cableado Estructurado.

3.4.1.2 Clasificación de la información

Objetivo de Control: Asegurar que los activos de información reciban el nivel de protección apropiado.

Guías de clasificación

El administrador de red debe manejar y proteger la información con respecto a la configuración, administración de los equipos activos de red, esta información debe ser bien elaborada organizada y clasificada de manera que se pueda tener

un control exhaustivo y esté disponible únicamente para personal clasificado.

3.5 SEGURIDAD LIGADA AL PERSONAL

3.5.1 Seguridad en la definición de cargos y suministros de recursos.

Objetivo de control: Reducir los riesgos de error humano, robo, fraude, o uso inadecuado de los equipos activos de red.

3.5.1.1 Selección y política sobre personal

En el momento que se reciben las solicitudes de trabajo para el Departamento de Tecnología de la Información y Comunicaciones se debe verificar los siguientes controles:

- Referencias satisfactorias laborales.
- Referencias satisfactorias personales.
- Comprobación de la precisión de la hoja de vida del candidato.
- Confirmación de las certificaciones académicas y profesionales.
- Comprobación independiente de la identificación.

El trabajo de todo el personal debe revisarse periódicamente y aprobarse sus procedimientos por personal de más categoría.

El jefe del departamento debe conocer que circunstancias privadas de su personal pueden afectar su trabajo. Los problemas personales o financieros , los cambios de su comportamiento o estilo de vida, las ausencias recurrentes y la depresión o el estrés evidentes podrían llevar a fraudes, robos, errores u otras implicaciones de seguridad en la red.

3.5.1.2 Acuerdos de confidencialidad.

Se deben usar acuerdos de confidencialidad para notificar que información es confidencial. Los empleados deben firmar normalmente una cláusula de confidencialidad como parte de su contrato de trabajo.

El HE-1 debe requerir el acuerdo de confidencialidad con personal temporal y los usuarios que son terceras partes no cubiertos por un contrato de trabajo, antes de su acceso a los equipos activos de red.

3.5.2 Respuestas a incidentes y anomalías en materia de seguridad de la red.

Objetivo de control: Minimizar el daño causado por incidentes y anomalías en materia de seguridad de red, hacer el seguimiento y aprender de estos incidentes.

3.5.2.1 Reporte de los incidentes de seguridad de la red.

Reportar a través del canal respectivo (Jefatura del Departamento de sistemas del HE-1), tan rápidamente como sean posibles caídas de la red, des configuraciones de los equipos de activos de red,

3.5.2.2 Reporte de las anomalías del software de red.

- Anotar los síntomas del problema y todo mensaje que aparezca en pantalla.
- Aislar el computador, si es posible y parar su uso.
- No se debe transferir discos a otros computadores.
- Informar inmediatamente al administrador de red.

3.5.2.3 Aprendizaje de los incidentes

Cuantificar cuanto representa una caída de la red en lo que respecta a descargos de insumos médicos, procedimientos que se perdieron por efecto de esta anomalía, hacer un seguimiento. A fin de identificar aquellos que se produzcan con mayor frecuencia o que tengan un fuerte impacto y mejorar o ampliar controles para limitar la frecuencia de estos.

3.5.2.4 Proceso disciplinario

- Los empleados que violen las políticas y procedimientos de seguridad de la red serán sancionados de acuerdo a los reglamentos en vigencia, de acuerdo a la gravedad del impacto que causaré, inclusive de responsabilidad económica y judicial.
- Personal que violare las políticas y procedimientos de seguridad de la red serán sancionados de acuerdo a los reglamentos de disciplina militar en vigencia.

3.6 SEGURIDAD FÍSICA Y DEL ENTORNO

3.6.1 Áreas seguras

Objetivo de control: Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones del data center del H.E-1.

3.6.1.1 Controles de acceso físico

- Tanto el data center principal como el alterno están protegidos por controles de entrada apropiados que aseguran que solo se permite el acceso a personal autorizado.

- El administrador de red es el responsable de la creación, actualización y registros del personal autorizado al ingreso de estas áreas.
- Los ingresos a estas áreas deben ser registrados en una bitácora por parte del administrador de red del HE-1

3.6.2 Seguridad de los equipos.

Objetivo de control: Evitar daño, pérdida o des configuración de los activos de los equipos activos de la red del HE-1

Controles:

3.6.2.1 Ubicación y protección de los equipos

Los equipos donde se procesa información deben estar ubicados y protegidos de amenazas como inundaciones, accesos no autorizados, robos.

- Se debe disponer del respectivo rack por cada piso para los equipos activos de red.
- Disponer de un Data Center que cumple normas y estándares que aseguran su correcto funcionamiento y además se implemente una topología de red a fin de lograr una alta disponibilidad de la infraestructura de red del HE-1.

3.6.2.2 Suministro de energía

Los equipos activos de red deben estar protegidos contra falla en el suministro de energía y otras anomalías eléctricas para lo cual el edificio de hospitalización cuenta con una red de energía estabilizada con sus respectivas normas y estándares a cumplir para este tipo de red eléctrica, y está destinada para

- Usuarios de la red de datos del HE-1 (personal de enfermeras, médicos residentes y tratantes que inter actúan con el sistema de gestión hospitalario en los diferentes pisos y servicios).
- Rack de comunicaciones por piso.
- Equipos activos de red (data center).

Esta red está sustentada por un sistema de UPS así como un generador eléctrico a fin de que garantice la estabilidad eléctrica que se requiere.

3.6.2.3 Seguridad del cableado

- El cableado de energía eléctrica y de telecomunicaciones que llega al centro de datos tiene medidas alternativas de protección como son la de ser tendidas a través de tubería metálica con sus respetivos ductos.
- La red de cableado estructurado en el HE-1 tiene las siguientes características:

La interconexión entre los dos bloques de edificios del HE-1 (Hospitalización y Administrativo) es de fibra óptica de 10 gigabits, tipo OM3 de 24 hilos.

Para el cableado de datos, el cable a utilizar es de categoría 6A S/FTP, 650 Mhz, chaqueta LSZH.

Todos los elementos del hardware de conexión y cable de telecomunicaciones cuentan con las certificaciones y pruebas para el canal de 100 m. categoría 6A, a 500MHz.

El Sistema de Cableado Estructurado debe está diseñado de manera que permite implementar un sistema integrado y transparente a todas las necesidades de comunicaciones (voz, datos, video y servicios de automatización).

El Cableado Estructurado contempla los siguientes subsistemas:

- Área de trabajo.
- Cableado Horizontal.
- Rack de Telecomunicaciones.

Ductos y canalizaciones

- Los ductos y canalizaciones están construidas con canaletas profesionales que cumplan con todos los requerimientos de TIA/EIA 569A con énfasis en que los radios de curvatura mínima de estos que deben tener es de 4 veces el diámetro del cable a utilizar (S/FTP CAT 6 A 4 pares).
- Sobre el cielo falso, en cada corredor de extremo a extremo, está instalado canaleta tipo bandeja ranurada, en cada uno de los pisos del edificio, aunque no existieran puntos de red a instalarse en aquellos sitios, con la finalidad de que quede dimensionada para futuras instalaciones, crecimientos
- El enrutamiento del cableado de datos en cobre y fibra óptica sobre el cielo falso está a través de la canaleta tipo bandeja en todo su recorrido hasta llegar al rack de cada piso.
- Todas las vías de cableado horizontales están instaladas y conectadas a tierra para cumplir los reglamentos eléctricos y de construcciones aplicables, nacionales y locales.
- La puesta y unión a tierra está de acuerdo con el estándar ANSI-J-STD-607-2002 ”CommercialBuildingGrounding (Earthing) and BondingRequirementsforTelecommunications” y unido al sistema de tierra existente.

3.6.2.4 Mantenimiento de los equipos activos de red

- Los equipos se deben mantener de acuerdo a las recomendaciones y especificaciones del equipo y del proveedor.
- Solo el personal técnico de administración de redes está autorizado a dar el respectivo mantenimiento preventivo.
- Llevar bitácoras a fin de llevar los registros de mantenimientos preventivos y correctivos y además de sospechas de fallas y fallas reales.

3.7 GESTIÓN DE COMUNICACIONES Y OPERACIONES

3.7.1 Procedimientos operacionales y responsabilidades.

Objetivo de control: Asegurar la integridad, confidencialidad y disponibilidad de la información en su trasmisión y recepción en la red de datos del HE-1

Normas y procedimientos de operación:

- Se documentarán y mantendrán actualizados los procedimientos operativos identificados en esta política y sus cambios serán autorizados por el Oficial de Seguridad.
- Los procedimientos especificarán instrucciones para la ejecución detallada de cada tarea, incluyendo:
  - Respaldos de red.
  - Recuperación de información
  - Control de cambios
- En cada uno de los procedimientos se deberán especificar cuáles son los

responsables de realizar las tareas en cada procedimiento.

3.7.1.1 Respaldos

- Los administradores del servicio de red deberán mantener documentos actualizados de políticas y manuales de administración, configuración y manejo de la red, así como software instalado en los servidores y equipos de comunicación, y usuarios finales para la adecuada administración de los mismos. Estos documentos deberán especificar:

    - Fecha de creación
    - Versión del documento
    - Cambios efectuados
    - Datos informativos de la persona que los elaboró
    - Aprobación
    - Ubicación Física

- Es de responsabilidad de los administradores de la red de mantener los documentos de políticas y manuales de los servicios en ambientes seguros y ponerlo en conocimiento de los dueños de datos de su área de trabajo.
- El departamento de Desarrollo Tecnológico debe proveer a los administradores de servicios un sistema de respaldos como: DVD, cintas, servidor de respaldos y evitar disponer de discos del almacenamiento externo para almacenar información de la Red del HE-1.
- Discos de respaldo externos que hayan sido entregados a un área del HE-1 deberán

ser de responsabilidad del dueño de datos el que deberá mantener un control de la información contenida en un proceso de eliminación de archivos no útiles para la Institución o información personal que pudiera estar almacenada. Estos discos estarán disponibles en caso de realizarse una auditoría de datos por parte de la autoridad competente.

- Los administradores de la red y base de datos, deberán respaldar datos, base de datos, configuraciones antes de aplicar cualquier cambio a las configuraciones de los equipos activos de red. Cada respaldo deberá mantener la fecha efectiva de respaldo, el objeto por el cual se da el respaldo, y la persona encargada del mismo.
- Solo los administradores de la red tiene acceso al lugar de almacenamiento de los respaldos en el HE-1. Deberá habilitarse una bitácora de registro de acceso a estos archivos.
- Se deberá tener un lugar alterno para guardar los respaldos físicamente, este lugar debe estar fuera de las instalaciones del edificio del HE-1. El lugar alterno de respaldos deberá contar con la infraestructura, medidas de seguridad y ambientales necesarias para mantener una adecuada organización y clasificación de las copias de respaldos.
- El proceso de respaldo en cintas o medios magnéticos deberá tener una periodicidad en la obtención de respaldos para cada medio de almacenamiento a fin de evitar que dicho medio pueda deteriorarse.
- Al momento en que los medio de respaldos (cintas magnéticas, DVD’s, etc.) deban desecharse, estos deberán ser destruidos de forma segura lógica y

físicamente para evitar copias o recuperación de la información almacenada.

- El administrador principal de red y su backup deberán realizar pruebas periódicas para verificar la validez y funcionalidad de las copias de las configuraciones de respaldo de todos los equipos activos de red.
- Toda la información respaldada será clasificada y etiquetada. En su medio de almacenamiento debe incluir: nombre del archivo, versión, aplicación o sistema al que pertenece la información, fecha de respaldo, persona que hizo el respaldo, ubicación física para su almacenamiento.

3.7.1.2 Control de cambios

Se deberá cumplir el proceso de control de cambios para cualquier cambio que se requiera realizar en: infraestructura, sistema, configuración en servidores, WAN, LAN y la incorporación de nuevos servicios tecnológicos.

- Se definirán procedimientos y estándares para cada área de TI para el control de los cambios en los ambientes operativos y de comunicación. Todo cambio deberá ser evaluado en aspectos técnicos y de seguridad.
- El Oficial de Seguridad de Información controlará que los cambios en los componentes operativos y de comunicación no afecten la información y seguridad de los mismos.
- Los procedimientos de control de cambios deberán contemplar lo siguiente:
  - Identificación y registros de cambios significativos.
  - Evaluación del posible impacto.
  - Evaluación de riesgos.

- Aprobación formal de los cambios propuestos.
- Planificación del proceso de cambios.
- Pruebas del nuevo escenario.
- Comunicación de cambios a todos los involucrados.
- Regirse a la Política de Control de Cambios establecida
- Identificación de las responsabilidades por la cancelación de los cambios fallidos y la recuperación respecto a los mismos.

3.7.1.3 Separación de los recursos de red, desarrollo pruebas y operación

Los ambientes de desarrollo, prueba y operaciones, siempre que sea posible, estarán separados preferentemente en forma física, y se definirán y documentarán las reglas para la transferencia de software y migraciones desde el estado de desarrollo hacia el estado operativo. Para ello, se tendrán en cuenta los siguientes controles:

- Separar la infraestructura de desarrollo y de operaciones, en diferentes ambientes de operaciones, equipos, y/o directorios.
- Separar las actividades de desarrollo y prueba, en entornos diferentes.
- Impedir el acceso a los compiladores, editores y otros utilitarios del sistema en el ambiente operativo, cuando no sean indispensables para el funcionamiento del mismo.
- Utilizar sistemas de autenticación y autorización independientes para los diferentes ambientes, así como perfiles de acceso a los sistemas. Prohibir a los usuarios compartir contraseñas en estos sistemas. Las interfaces de los sistemas identificarán claramente a qué instancia se está realizando la

conexión.

- Definir propietarios de la información para cada uno de los ambientes de procesamiento existentes.
- Las personas que trabajen en el desarrollo de aplicaciones o en el ambiente provisto para ello no tendrá acceso al ambiente operativo. De ser extrema dicha necesidad, se establecerá un procedimiento de emergencia para la autorización, documentación y registro de dichos accesos.
- El uso de datos reales en los ambientes de prueba deberán considerar un **proceso de limpieza de datos** previa a fin de no exponer información de Propiedad Intelectual o aquella con un nivel de

3.7.1.4 Confidencialidad

Todo servicio deberá ser probado y verificado su funcionamiento en un ambiente de pruebas.

3.7.2 Administración de redes.

Objetivo de control: Asegurar la protección de la información de las redes y la protección de la infraestructura de soporte.

Controles:

3.7.2.1 Controles de redes

- El área de administración de redes debe estar separada de las otras áreas del departamento de sistemas de HE-1.

- El administrador de red es el responsable de la gestión de los equipos activos de red, esto es su organización, administración y mantenimiento.
- Se debe realizar un monitoreo permanente

3.8 Control de acceso

3.8.1 Administración de acceso a usuarios a la red.

Objetivo de control: Evitar acceso no autorizados a la red informática.

Controles:

3.8.1.1 Registro de Usuarios

- Una vez creado el perfil, el usuario tendrá asignado un nombre único de usuario y contraseña para acceder a los sistemas informáticos permitidos según su perfil. Si existe alguna excepción, esta debe ser autorizada por el administrador de base de datos en conocimiento por el Jefe del Departamento de Tecnologías de la Información del HE-1
- Comprobación de la validación del usuario y contraseña a través de un Active Directory.
- Entrega de manera formal impreso a cada usuario respectivamente.
- Mantenimiento de un registro formalizado de todos los registros de manera permanente.
- Revisión periódica y eliminación de cuentas de usuario que han salido del HE-1 por diferentes motivos: renuncia voluntaria, separación de esta casa de salud, periodo de cursos en el exterior, etc.

- El otorgamiento de roles y perfiles de usuario deberá ser definido de acuerdo al principio del mínimo privilegio.

3.8.1.2 Administración de privilegios

- Cada director, empleado o agente externo debe estar asociado a un rol/perfil en los sistemas informáticos de acuerdo a las actividades que realiza. Y cada aplicación debe gestionar el nivel de privilegios que tienen los usuarios dentro del sistema informático.
- Es responsabilidad de los administradores de servidores y servicios, la correcta administración de las cuentas de acceso, el otorgamiento de privilegios de acuerdo a las autorizaciones que se especifiquen en el flujo de autorización.
- Una vez que el funcionario deja sus funciones al interior del hospital, la salida debe ser notificada por el Departamento de Recursos Humanos hacia el Jefe de Desarrollo Tecnológico, Administrador de base de datos, posterior a lo cual se revocan todos los permisos asignados a dicho usuario, y se retiran los equipos tecnológicos asignados.
- Si un funcionario cambia de departamento de trabajo al interior del hospital, el cambio debe ser notificado por el Departamento de Recursos Humanos hacia el Jefe de Desarrollo Tecnológico, Administrador de Base de Datos posterior a lo cual se revocan los privilegios asociados a sus funciones y se realiza el proceso de asignación de activos nuevamente, con lo cual el equipo debe ingresar al Departamento de Desarrollo Tecnológico para su limpieza, formateo y respaldo.
- Si un funcionario bajo solicitud del Dueño de Datos debe mantener sus privilegios

actuales ante un cambio de departamento de trabajo, esta aprobación deberá autorizarla el Director de Recursos Humanos y en conocimiento del Jefe de Desarrollo Tecnológico, posterior a lo cual se revocarán los permisos otorgados y se procederá como se especifica en el punto anterior.

3.8.1.3 Administración de contraseñas para usuario

Las contraseñas son medios de uso corriente que validan la identificación de un usuario para acceder a un sistema.

- El manejo de contraseñas es de responsabilidad del usuario una vez que han sido entregadas, por lo que la pérdida o divulgación de las mismas es responsabilidad del usuario, está prohibida la publicación escrita de las mismas a través de medios fácilmente identificables.
- La notificación de las contraseñas por parte de los administradores se realizará vía impresa con una firma de aceptación por parte del funcionario quién recibe el acceso.
- Se debe aplicar un estándar de creación de contraseñas seguras para el acceso de usuarios finales a los diferentes sistemas, el que contendrá parámetros mínimos en el manejo de las mismas por parte de los usuarios.
- Se debe aplicar el estándar de creación de contraseñas seguras para el acceso a la administración de los sistemas, servidores o equipos de comunicación, el que contendrá parámetros mínimos en el manejo de las mismas por parte de los administradores de los sistemas.
- Una vez proporcionadas las credenciales de accesos a los sistemas, se debe

permitir al usuario el cambio de su clave obligatoriamente cuando ingresa por primera vez al sistema. Esta nueva clave guardará relación con el estándar de contraseñas seguras.

- Se debe utilizar un sistema de gestión de usuarios que permita:
  - Bloquear al usuario en la aplicación posterior a 5 intentos fallidos en el ingreso de sus credenciales.
  - Desbloqueo manual por el Administrador del sistema.
  - Cambiar la contraseña al menos cada **2 meses** para los usuarios finales y en el caso de los administradores de servicios, servidores o equipos de comunicación se deberá cambiar obligatoriamente esta contraseña cada **3 meses** manteniendo un registro de los últimos 6 cambios efectivos.
- Se debe cambiar inmediatamente la contraseña al sospechar o detectar que ha sido comprometida.
- Todo director, empleado o agente externo para el hospital debe mantener sus equipos de trabajo diario como: PC, PORTATIL con contraseña de acceso segura cuando no estén trabajando en ellas. Al momento de abandonar su estación de trabajo tendrán la obligación de bloquear su equipo.

3.8.1.4 Seguimiento y Auditoría

- Se deberá activar el registro de auditoría en los servicios, servidores, equipos de comunicación y sistemas críticos, para los diferentes usuarios del sistema incluyendo aquellos con privilegios administrativos. Dichos registros de auditoría no deben generar carga operativa en los equipos que afecte su correcto y normal

funcionamiento.

- Los registros de auditoría deberán ser eliminados periódicamente, posterior a obtener un respaldo físico de los mismos en caso de encontrar alguna irregularidad, esto a fin de no afectar el rendimiento de los equipos.

3.8.2 Responsabilidades de los usuarios de la red

Objetivo de control: Evitar el acceso de usuarios no autorizados a la red.

Controles:

3.8.2.1 Uso de contraseñas

- Mantener la confidencialidad de las contraseñas.
- Evitar la escritura de las contraseñas en papel.
- Cambiar las contraseñas periódicamente.
- Seleccionar contraseñas de buena calidad, con una longitud mínima de 6 caracteres, fáciles de recordar, que no estén basadas en fechas de nacimiento, nombres, números de teléfono.

3.8.2.2 Equipo de cómputo de usuario desatendido

- Los usuarios deberán asegurarse que los equipos informáticos desatendidos estén debidamente protegidos.
- Cancelar todas las sesiones activas antes de abandonar la estación de trabajo.
- Proteger el terminal o el puesto de trabajo, cuando no estén en uso con una contraseña de acceso.

3.8.3 Control de accesos a redes.

Objetivo de control: Protección de los servicios en red

Controles:

3.8.3.1 Autenticación de usuarios para conexiones externas

Las conexiones externas (por línea telefónica, modem, por internet), son una fuente potencial de accesos no autorizados a la red del hospital.

- Se debe autenticar a los usuarios remotos a través de una contraseña.
- Se debe registra en una bitácora todos los accesos a la red.

3.9 CONCLUSIONES

El Ministerio de Defensa Nacional en el mes de marzo del 2012, dispone al Hospital de Especialidades de FFAA a través del COMACO la implementación del Sistema Informático de Gestión Hospitalaria para Fuerzas Armadas, ante este hecho el hospital en lo que respecta a la red existente se encontraba en la siguiente situación:

- En la infraestructura de la red hospitalaria, el Back bone vertical en el edificio de hospitalización, era únicamente de Cu, limitando así la capacidad de comunicaciones en la trasmisión de datos a una velocidad máxima de 1 Gbps, durante el desarrollo de este proyecto se logró implementar dicho Back bone con Fibra óptica, ampliando el canal de comunicación a 10 Gbps.
- La red LAN hospitalaria no disponía de racks de comunicaciones por piso, disponiendo de un rack de comunicaciones para 3 o 4 pisos, lo que complicaba sustancialmente la administración y la explotación de la red, al existir una falla

eléctrica en el piso donde existía el rack de comunicaciones implicaba que los tres pisos se queden sin red. Hoy ya se cuenta con racks por cada piso.

- Durante este proyecto el Hospital de Especialidades de FFAA ha mejorado la infraestructura de red abriendo ventanas para la nueva tecnología hospitalaria como la telemedicina, Sistema radiológico en red, Imagen, sistema informático de gestión hospitalaria integral, quirófanos inteligentes, obteniendo de esta infraestructura de red: interoperabilidad, convergencia, escalabilidad, alta disponibilidad, seguridad y movilidad.
- Se encontró un crecimiento desordenado de la red de datos y un parque de computadores por cada proyecto de manera individual, sin un enfoque global.
- En cada piso de hospitalización existía máximo una computadora en la estación de enfermería, no existía un sistema de cableado estructurado ni tampoco una red de energía estabilizada.
- Se disponía únicamente de un cuarto de equipos en donde se encontraban instalados los equipos activos de red los mismos que soportaban la red de datos hospitalaria sin una adecuada infraestructura tecnológica poniendo en alto riesgo la operatividad de la misma.
- Se implementó un nuevo data center bajo las normas y estándares que rige la tecnología, brindando una adecuada instalación con control de accesos, sistema de climatización, sistema de energía estabilizada.
- Este trabajo plantea una política de seguridad para una red segura, basada en la norma ISO 17799.

- Durante el desarrollo de este proyecto se ha ejecutado proyectos para la mejora de la infraestructura de red hospitalaria sobre el millón de dólares.
- Los beneficios de estos proyectos ya se ven reflejados en la mejoría de atención a los pacientes, así como también lograr disponer de un sistema de gestión integrando la parte administrativa, médica y tecnológica

3.10 RECOMENDACIONES

- La infraestructura de red alcanzada con este proyecto es muy importante para el hospital y con el apoyo permanente y comprometido de la Dirección General, se requiere la disponibilidad de profesionales capacitados que cumplan con las funciones de administradores de redes y base de datos, que tengan nombramiento en esta casa de salud, ya que al momento no existe este personal con estabilidad laboral y se vuelve en una debilidad que podría comprometer la operatividad de la red segura.
- Apoyar al comité conformado para la seguridad de la red, a fin de que se cumplan sus funciones y responsabilidades establecidas en este trabajo y puedan ejecutar el ciclo de mejora continua, a fin de brindar integridad, confiabilidad y disponibilidad de la información que sea transmitida por la infraestructura de red hospitalaria.

- Obtener una autorización institucional de la Política de Seguridad para la Red Segura, planteada en este proyecto a fin de cumplir los objetivos institucionales.

CAPÍTULO I V

IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN HOSPITALARIO

4.1. ESTRUCTURA DEL SISTEMA.

El Sistema Informático de Gestión Hospitalario está compuesto de los siguientes módulos:

a. Admisiones y emergencia.

b. Enfermería.

c. Expediente clínico electrónico.

d. Consulta externa.

e. Hospitalización e internamiento.

f. Cirugía.

g. Promociones, convenios y tarifarios.

h. Laboratorio patológico y citología.

i. Laboratorio clínico.

j. Imagenología.

k. Microbiología.

l. Gastroenterología.

m. Farmacia.

n. Sub bodegas.

o. Bodega central.

p. Endocrinología.

q. Inmunología.

r. Banco de sangre – serología.

s. Administración.

t. Auditoria médica.

u. Facturación y cartera.

Para una mejor comprensión dela aplicación del software a implementarse en esta casa de salud se hace un análisis del diagrama que permite identificar los macro procesos del Hospital de Especialidades de FFAA, y describe sus interrelaciones principales.

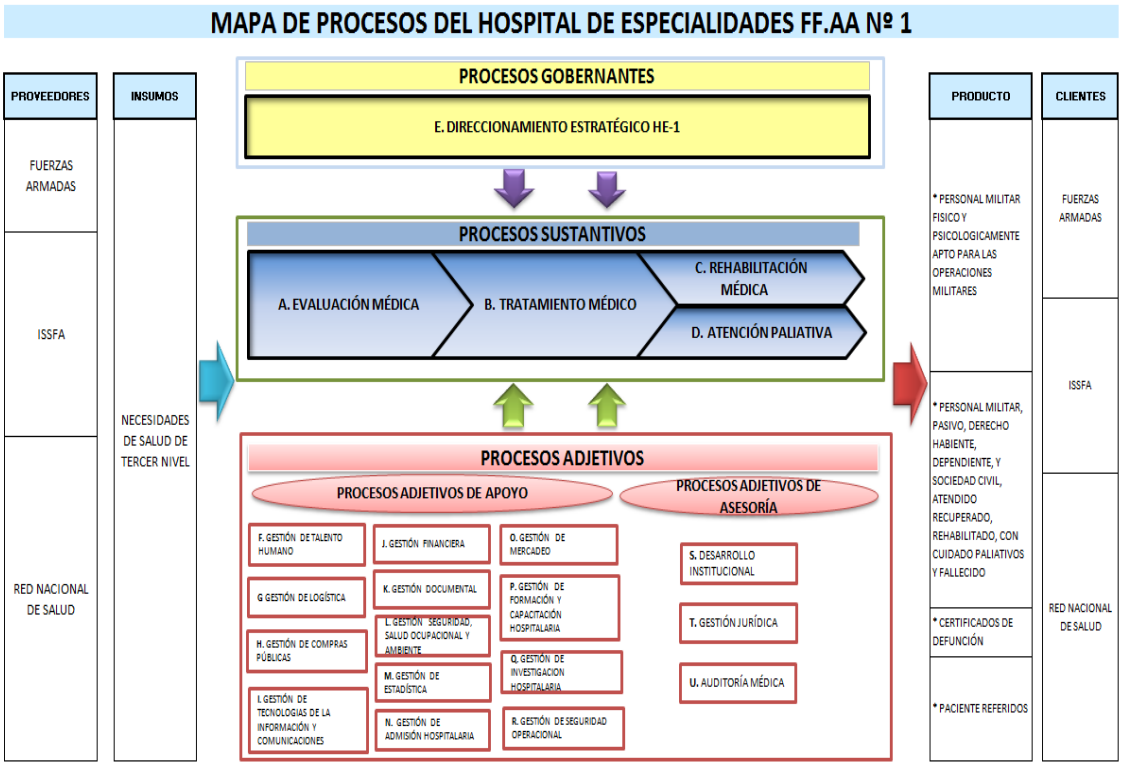
Los tipos de macro procesos que se describen en el mapa de procesos son: procesos gobernantes, procesos sustantivos y procesos adjetivos, como se indica en el gráfico 4.1, los **MACROPROCESOS SUSTANTIVOS** como:

- **EVALUACIÓN MÉDICA.-** Establece el diagnóstico presuntivo o definitivo a través del análisis y la valoración de los pacientes en la especialidad correspondiente a los síntomas presentados.

- **TRATAMIENTO MÉDICO.-** Aplicación clínica, quirúrgica y especial que permita reducir o eliminar los síntomas de enfermedad detectados en la evaluación médica.

- **REHABILITACIÓN MÉDICA.-** Recuperación física y/o mental parcial o total del paciente.

- **ATENCIÓN PALIATIVA.-** Seguimiento y control médico, psicológicos,



emocional de un paciente en etapa terminal y a su familia.

Gráfico 4.1: Mapa de procesos del HE-1

Y es a estos procesos que el Sistema Informático de Gestión Hospitalario automatizará, que los podemos relacionarlos directamente a los siguientes procesos de acuerdo a la Tabla 4.1:

Tabla 4.1: Relación módulo / proceso

Módulo del SGH	Proceso de Apoyo	Literal del proceso
Admisión y Emergencia	Gestión de admisión hospitalaria	N
Enfermería	Rehabilitación médica	C

Expediente Clínico Electrónico	Evaluación médica	A
Consulta Externa	Evaluación médica y rehabilitación médica	A , C
Hospitalización e Internamiento	Tratamiento médico	B
Cirugía	Tratamiento médico	B
Promociones convenios y tarifarios	Gestión financiera	J
Laboratorio Patológico y Citología.	Evaluación médica	A
Laboratorio Clínico	Evaluación médica	A
Imagenología	Evaluación médica	A
Microbiología	Evaluación médica	A
Gastroenterología	Rehabilitación médica	C
Farmacia	Gestión de logística	G
Sub bodegas	Gestión de logística	G
Bodega Central	Gestión de logística	G
Endocrinología	Evaluación médica y rehabilitación médica	A,C
Inmunología	Evaluación médica y rehabilitación médica	A,C
Banco de Sangre- serología	Tratamiento médico	B

Administración	Gestión de talento humano.	F
Auditoría Médica	Auditoría médica	U
Facturación y Cartera	Gestión financiera	J

Pantalla de inicio donde se muestra los módulos del Sistema de Gestión Hospitalaria:

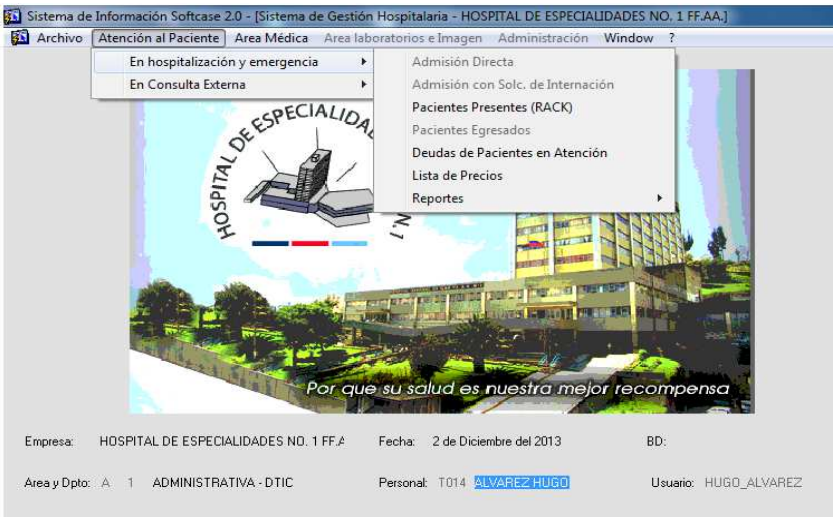


Gráfico 4.2: Módulos del Sistema de Gestión Hospitalario

Entre los principales módulos se muestra el de hospitalización y Emergencia y tienen las siguientes opciones como se muestran en el gráfico 4.3.

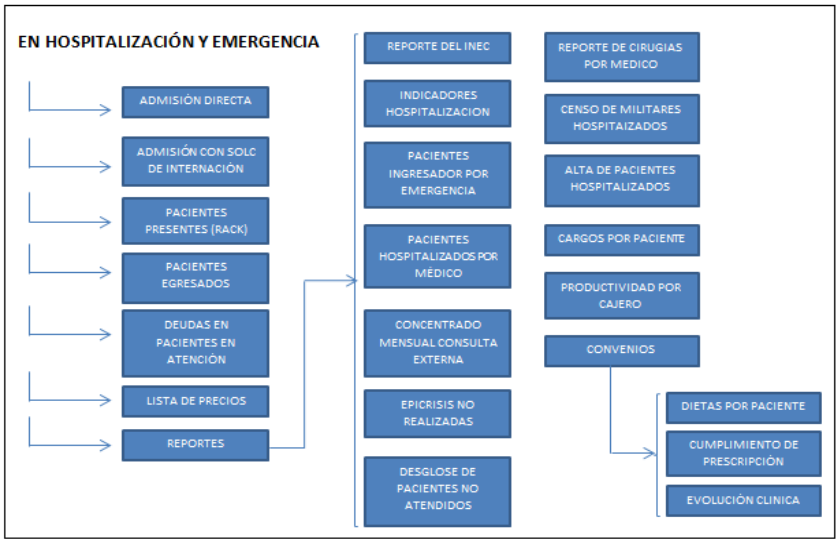


Gráfico 4.3: Módulos de Hospitalización y Emergencia

El módulo de Consulta Externa tiene las siguientes opciones como se muestra en el gráfico 4.4:

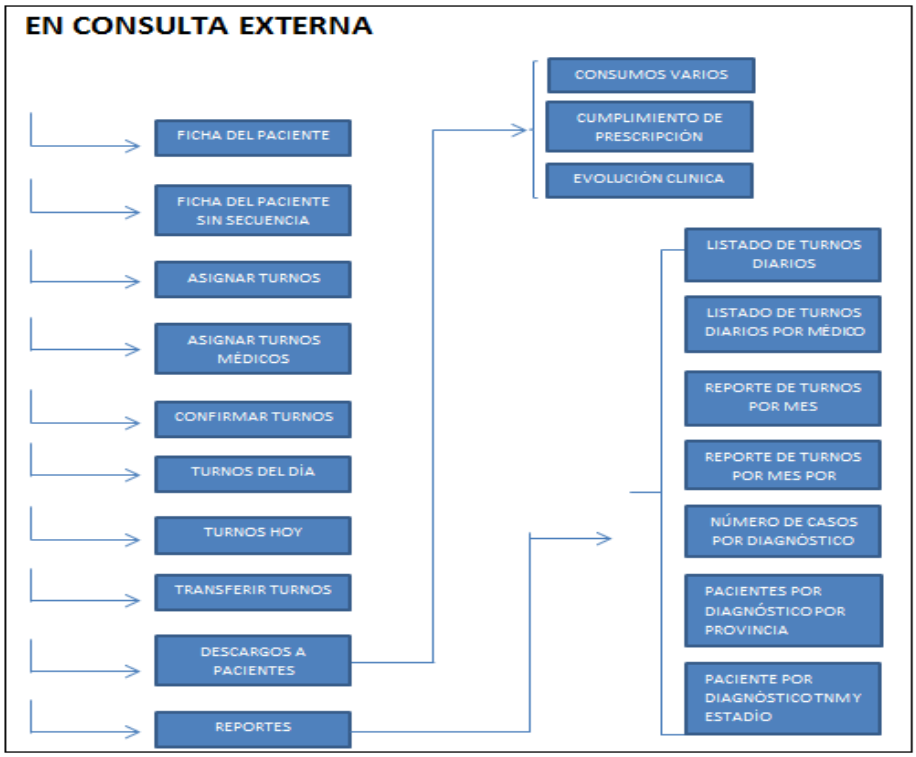


Grafico 4.4: Módulo de Consulta Externa

El módulo de Cirugía tiene las siguientes opciones como se muestra en el gráfico 4.5

Gráfico 4.5: Módulo de Cirugía.

El módulo de Laboratorio clínico muestra las siguientes opciones como se muestra en el gráfico 4.6

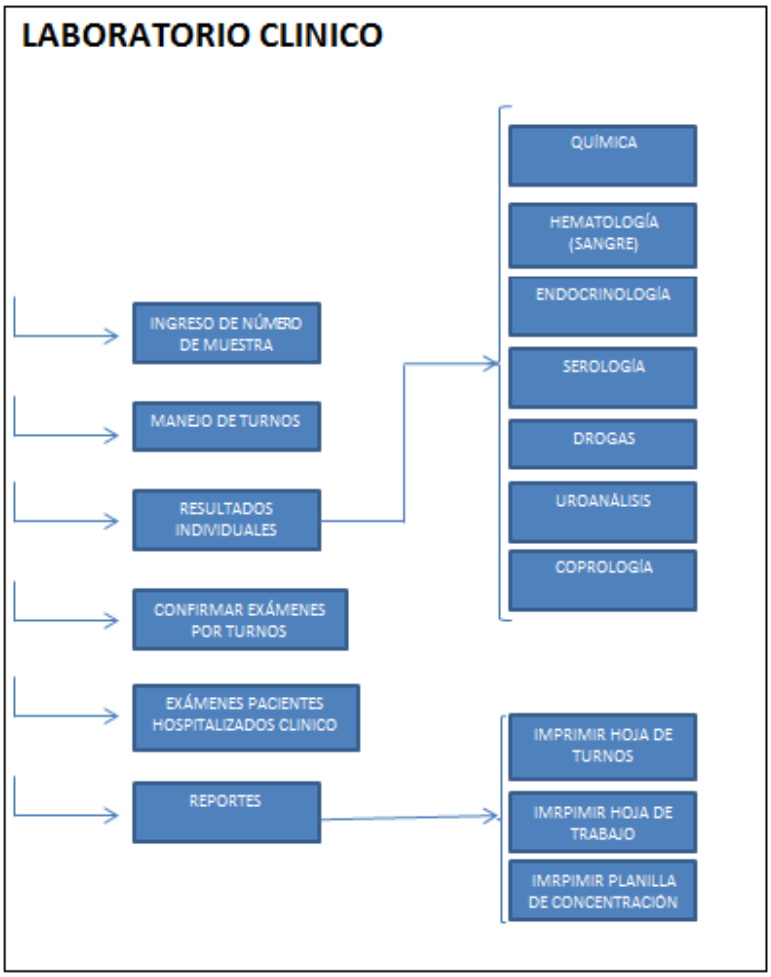


Gráfico 4.6: Módulos de Laboratorio clínico

4.2 AREAS INVOLUCRADAS EN LA IMPLEMENTACIÓN DEL SISTEMA

Las áreas involucradas para la Implementación del Sistema de Gestión Hospitalario son:

- **Director General y Director Médico** del Hospital de Especialidades de FFAA.
- **Área médica**: Auxiliares de enfermería, laboratoristas, Enfermeras, médicos residentes y tratantes.

- **Área Administrativa**: Bodegueros, secretarias, farmacéuticos, jefes y directores de los departamentos administrativos.
- **Área Financiera**: tesorería, contabilidad, crédito y cobranzas.
- **Área de Sistemas**: Equipo técnico de implementación (técnicos del HE-1 con técnicos de la empresa dueña del software), administrador de base de datos, administrador de red.

4.3 REQUERIMIENTOS DE INFORMACIÓN

Se vuelve de manera imperativa la toma física de inventarios, el respectivo ingreso de saldos de todas la bodegas (Insumos Médicos, laboratorio, insumos de oficina, insumos de limpieza, partes y repuestos y bodega general).

De manera impostergable y obligatoria, se debe realizar el conteo físico y respectivo ingreso de las especies existentes (insumos médicos), por medio del mecanismo de regulación de inventarios en todas las sub bodegas de los pisos de hospitalización incluyendo las bodegas de Unidad de Cuidados Intensivos y Emergencia.

Durante el proceso de conteo físico y registro de información del sistema, se verificó que todos los ítems que se encuentran en las bodegas posean la respectiva etiqueta de códigos de barras. En caso de existir ítems que no posean estas etiquetas, se procedió al etiquetado de estos ítems o su remplazo por ítems similares que contengan estas etiquetas.

La toma física de inventarios y el respectivo ingreso de saldos de la bodega general de fármacos con su respectivo costo, es muy importante.

El tipo de información analizada para la migración de datos fue básicamente:

- Información de pacientes (Nombre, sexo, edad, tipo de paciente militar servicio activo, pasivo).
- Insumos médicos.
- Suministros.
- Usuarios del sistema (médicos, enfermeras, administrativos).

Es importante informar por escrito de la culminación de estos procesos, para que el equipo técnico de implementación migre la información requerida.

4.4 ESTRATEGIA DE IMPLEMENTACION

La implementación de la estrategia involucra a todas las funciones y personas de esta casa de salud, pero al ápice estratégico le corresponde evaluar y liderar los tres elementos esenciales de este proceso: **elcambio estratégico, la estructura formal e informal y la cultura**. Por lo antes expuesto se considera que el papel del liderazgo de la Dirección General y su Equipo Técnico de Implementación es decisivo en la dirección estratégica ya que los resultados positivos o negativos dependen de ello.

Se decide una implementación por fases iniciando en el área de Emergencia, luego en el área de Hospitalización (por pisos) y finalmente en Consulta externa.

Tanto para la implementación del sistema en las áreas definidas anteriormente se debe mantener de manera paralela el sistema a ser reemplazado, hasta verificar la validez de los procesos e información que sean ejecutados, esto demandó un doble esfuerzo por parte del personal médico sobre todo el área de enfermería.

Esta estrategia está basada en cuatro pilares fundamentales que son:

4.4.1 INFRAESTRUCTURA TECNOLÓGICA:

Antes del proyecto, se encontró al hospital con una infra estructura de red que no brindaba las garantías del caso para la implementación del sistema informático, equipamiento informático insuficiente (PCs, impresora, pistolas de código de barras, etc).

Una vez implementada toda la infraestructura de red como es cableado estructurado, red de energía estabilizada, nueva topología de red, nuevo data center y además de haber estructurado una red segura en base a la ISO 17799, el hospital quedó en condiciones de iniciar su implementación del sistema de gestión hospitalario.

Se ejecutó un plan de atención a usuarios durante la implementación activando un número de teléfono de la red interna asignado el 1700 (HelpDesk), y apoyado con una red de comunicación convencional VHF por el personal técnico del HE-1

4.4.2 CAPACITACIÓN

La capacitación se inició primero al personal técnico del hospital**,** luego a través de una selección del personal médico se formó un grupo líderes en los diferentes servicios y áreas, quienes a su vez adoptan la responsabilidad de capacitar, socializar a su personal y motivar de manera permanente a fin de lograr realizar este cambio del sistema y minimizar al máximo los impactos, como se detallada en el gráfico 4.7

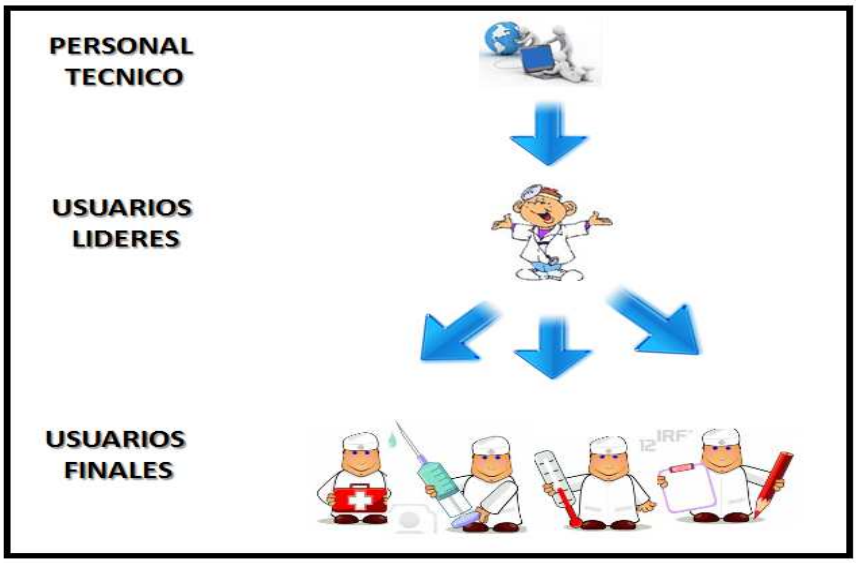


Gráfico 4.7: Proceso de capacitación.

Se implementó la herramienta del E-learnig en esta casa de salud, donde se puso en línea videos de capacitación desarrollados de la manera más didáctica socializando esta herramienta a fin de que cualquier usuario pueda acceder e iniciar su auto capacitación en este proceso de implantación inclusive desde su casa.

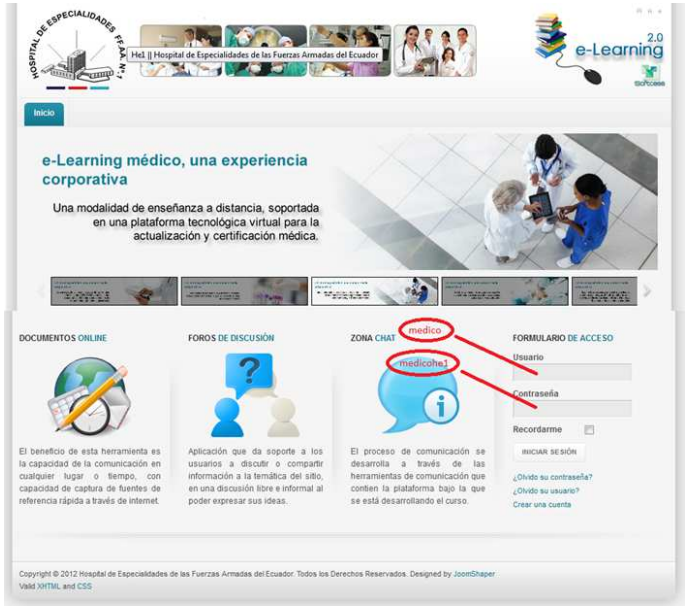


Gráfico 4.8: Portal para capacitación

4.4.2.1 CONTENIDO DE CAPACITACIÓN A USUARIOS LÍDERES

1. Introducción a la capacitación y explicación del proceso de implementación del Software de Gestión Hospitalaria.
2. Explicación de los procesos que tienen que ver con el Área que se está capacitando.
3. Explicación de la operatividad de las pantallas del sistema (Responsabilidad técnico encargado del área).
   a. Claves de Acceso
      - Significado y validación de las claves
      - Seguridades en el uso de las claves de acceso.
   b. Descripción de la pantalla inicial
      - Menú de opciones
      - Datos complementarios de la pantalla.
   c. Actualización / Cambio de claves de acceso
      - Técnicas para generar claves de usuario
      - Tiempos de renovación de las claves.
   d. Estructura de la pantalla
      - Menú de opciones
      - Funcionalidad de las teclas
      - Mensajes del sistema (Cuadros de texto / barra de mensajes)
      - Búsquedas (Directas / Uso de Comodines / Búsquedas Compuestas)
      - Uso de combos

- Uso de listas
- Campos obligatorios.

e. Explicación de cómo acceder a videos de capacitación

f. Taller (Practicar búsquedas y familiarización con las teclas y menús del sistema).

4. Explicación de funcionamiento del módulo:

   a. Preparación de datos para capacitación (Datos a utilizar por cada usuario líder).

   b. Definición de técnicos para soporte en la capacitación y asignación de usuarios.

4.4.2.2 ACTIVIDADES PREVIAS A LA CAPACITACIÓN.

El encargado de la capacitación debe previamente coordinar y disponer:

1. Nómina de Usuarios lideres:

   a. Claves comprobadas.

   b. Listado para entrega de claves con firmas de responsabilidad.

2. Sistema funcionando desde una LAPTOP.
3. Verificación previa del funcionamiento del sistema.
4. Sistema de grabación de la capacitación activado.
5. Definir el encargado de tomar apuntes para la elaboración del acta de la capacitación.

6. Elaborar guía de capacitación y coordinar material didáctico necesario.

4.4.2.3 ÁREAS DE CAPACITACIÓN.

En el gráfico 4.9 se detalla todas las áreas que son parte del Hospital de Especialidades de FFAA que tiene participación en la implementación del Sistema de Gestión Hospitalario.

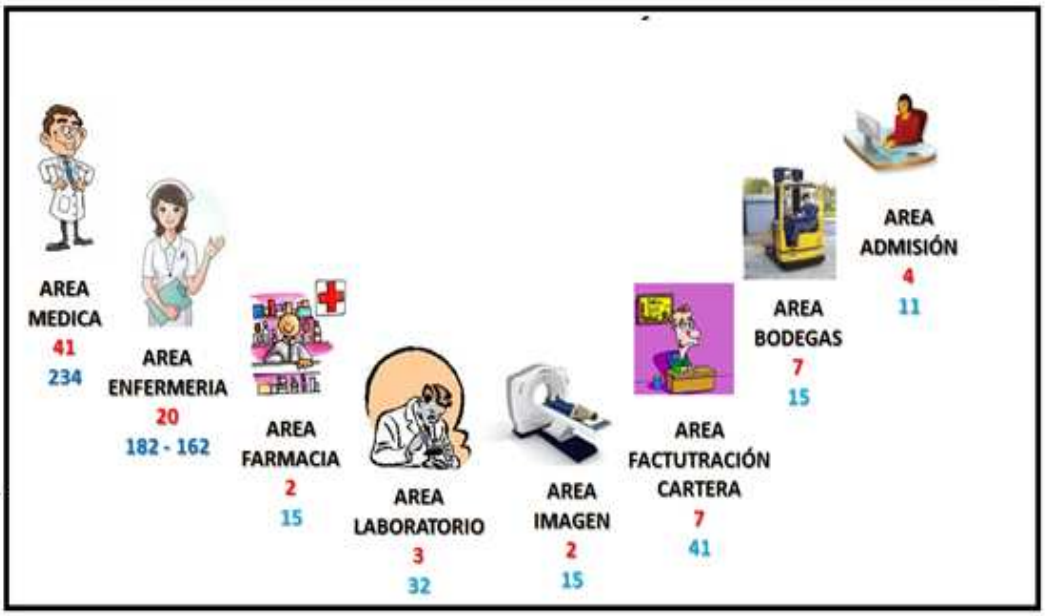


GRÁFICO 4.9: Áreas de capacitación.

4.4.2.4 GUÍA DE CAPACITACIÓN DEL SISTEMA DE GESTIÓN HOSPITALARIA AL PERSONAL MÉDICO.

La capacitación sobre el manejo de los módulos del Sistema de Gestión Hospitalaria que deben ser operados por el personal médico del hospital HE1, está dirigida en función al lugar en dónde está el paciente recibiendo atención médica.

Considerando que el sistema entra en producción en los servicios de Hospitalización y Emergencia partiremos con la explicación del manejo del sistema por parte de los médicos para brindar atención a pacientes admitidos para el servicio de Hospitalización y Emergencia y posteriormente continuaremos con la atención en Consulta Externa.

Los temas revisados durante el transcurso de la Capacitación fueron:

1. Explicación de la funcionalidad de la pantalla RACK.
2. Explicación de la estructura (3 cuadrantes) de la pantalla Hoja de Evolución Clínica en dónde se puede visualizar el expediente clínico del paciente.
3. Explicación de la funcionalidad y manejo del primer cuadrante que tiene la estructura de un árbol en la pantalla (Antecedentes Personales, Antecedentes Familiares, Antecedentes Gineco-obstétricos, Hábitos, Alergias).
4. Explicación del segundo cuadrante de la pantalla (Resumen de los procesos manejados en el expediente Clínico y Manejo de Diagnósticos del Paciente).
5. Explicación del tercer cuadrante (Evolución Clínica y procesos vinculados a la evolución mediante la activación de botones).
6. Explicación detallada de la función de cada botón que corresponden a las decisiones que toma el médico con respecto a la atención al paciente tales como:
    - Registro de Signos Vitales, Revisión de Sistemas, Exploraciones Físicas, Topo grama del paciente.
    - Solicitudes de exámenes de Laboratorio y Estudios de Imagen.

- Elaboración de Prescripciones Médicas (Perfiles, correlación con inventarios), solicitud de Valoraciones Cardiológicas.
- Solicitar Parte Operatorio.
- Solicitar Transfusiones
- Completar Parte Operatorio.
- Solicitar Interconsulta
- Responder Interconsulta por medio de Solicitudes Pendientes
- Realizar Procedimiento menor.
- Realizar Epicrisis.

7. Atención desde Consulta Externa mediante la lista de pacientes con turnos asignados para el médico.
   - Solicitar Internación de paciente.
   - Reservar turnos para atención subsecuente con el médico.
   - Control de Embarazo.
8. Taller práctico.

4.4.2.5 PROCESO DE CAPACITACIÓN.

La capacitación se describe básicamente en saber de manera clara que indica el

proceso del módulo en referencia, luego ingresar a este módulo en el sistema de gestión hospitalario e ir desplegando las bondades y funcionalidades de cada módulo a detalle como se indica a continuación en el gráfico 4.10.

GRÁFICO 4.10: Proceso de capacitación

4.4.2.6 CAPACITACIÓN DE LOS MÓDULOS.

La capacitación sobre el manejo de los módulos del Sistema de Gestión Hospitalaria que deben ser operados por el personal de enfermería médico y administrativo del hospital HE1, estuvo dirigida bajo la siguiente modalidad:

Introducción previa por parte del personal técnico de DTIC sobre la implementación del SIGH y revisión de la funcionalidad general de las pantallas de sistema.

Luego de la introducción, se explicó detalladamente la funcionalidad operativa de cada módulo que se puntualiza a continuación:

1. Explicación de la pantalla RACK (Pacientes en Atención).
2. Manejo de habilitación e inhabilitación de camas por parte de las supervisoras de pisos.
3. Pantalla de Censo diario de Pacientes (Hospitalizados)
4. Cómo actualizar el Censo Diario.
5. Cómo transferir a un paciente hospitalizado en un piso a una sala de manejo crítico como Neonatología, UCI y Unidad de Quemados.
6. Revisión de Hoja de Evolución Clínica realizada por los Médicos.
7. Registro de Hoja de Evolución de Enfermería.
8. Registro de Signos Vitales del paciente.
9. Registro de Ingesta y Eliminación de Líquidos.
10. Realizar Egresos de Sub bodegas.

11. Realizar Descargos Generales en el área de Emergencia y Quirófanos.
12. Realizar registro de Consumos Varios.
13. Solicitar Dietas.
14. Solicitar Descargos de Farmacia.
15. Descargos Generales (Emergencia y Quirófanos).
16. Registros de Enfermería.

- Planes de prueba.
- Puesta en marcha del sistema.

Una vez ingresado al sistema de gestión hospitalario, existe un flujo lógico de procedimiento en donde se valida su claves de acceso y se encuentra definido un rol por cada usuario como se indica a continuación en la gráfica 4.11.

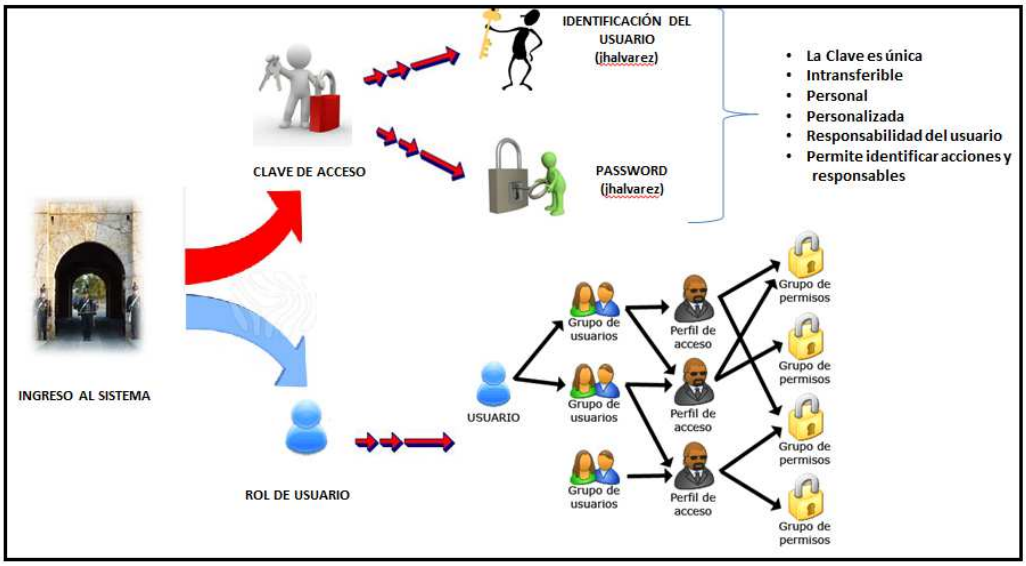


GRÁFICO 4.11: Ingreso al sistema

Para la implementación de este sistema el Equipo Técnico planificó una red de radio VHF y una red interna de telefonía asignando al número 1700 como el soporte

técnico en todo el proceso a iniciar como se muestra en la gráfica 4.12

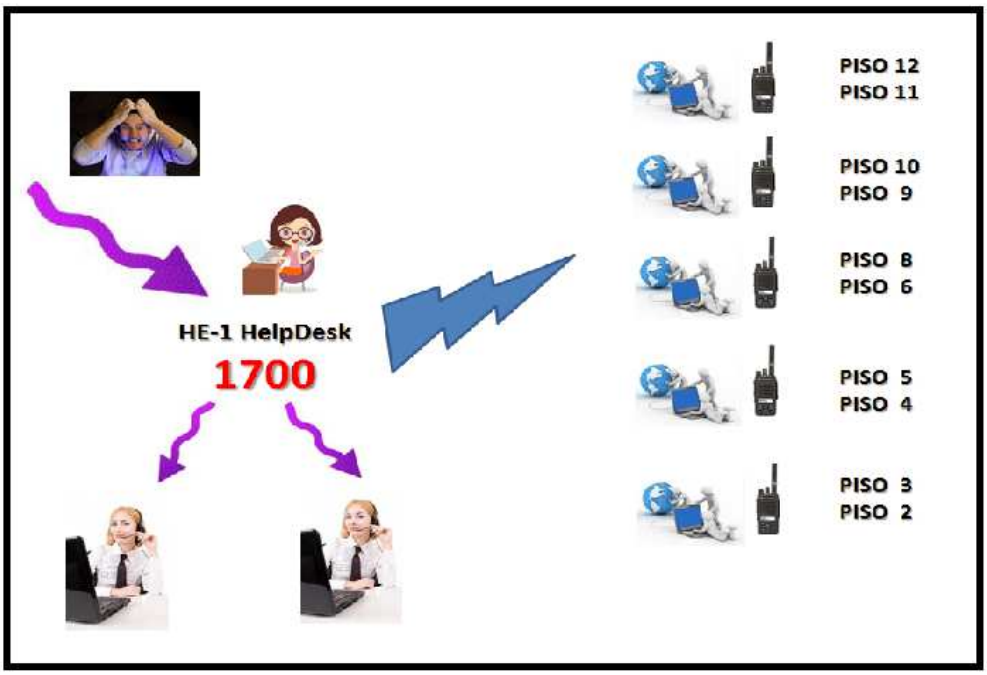


Gráfico 4.12: Red de radio VHF y red telefónica 1700

4.4.2.7 FASES PLANIFICADAS PARA LA IMPLEMENTACIÓN.

FASE 1	FASE 2	FASE 3
•Capacitación Personal Técnico •Capacitación Usuarios Lideres •Capacitación Usuarios Finales	•Implementación •Admisión y Emergencia •Hospitalización e Internamiento •Farmacia •Sub Bodegas •Bodega Central •Administración •Facturación •Cartera •Promociones y Convenios	•Enfermería •Expediente Clínico •Consulta Externa •Cirugía •Laboratorio •Imagenología •Gastroenterología •Endocrinología •Inmunología •Serología •Auditoría Médica

GRÁFICO 4.13: Fases planificadas para la implementación del SGH.

4.5 MANEJO DEL CAMBIO

4.5.1 LA FUNCIÓN DE LA DIRECCIÓN EN LA CONDUCCIÓN DEL CAMBIO.

El equipo técnico formado en esta casa de salud tuvo la oportunidad de vivir la confluencia de un liderazgo, ante una misión titánica construida desde los valores de las personas integrantes de este equipo y de un plan de acción compartido, estuvo en medio la unaoportunidad histórica de cambiar el hospital militar.

El equipo técnico multidisciplinario, movilizó al hospital en el cumplimiento para la implementación, el cual se empoderó con la misión institucional y traducida a objetivos estratégicos precisos y verificables pudo llegar al éxito de este proyecto.

Para el cumplimiento efectivo de la implementación del Sistema Informático de Gestión Hospitalario, el equipo directivo comprometió a todo el hospital para que responda efectivamente a las necesidades del cambio requeridas; se adapte con éxito a las nuevas condiciones del sistema, nuevas políticas y se cumpla con los objetivos planteados y requeridos por los servicios hospitalarios y se posicioneadecuadamente el nuevo sistema.

El proceso de cambio implicó grandes riesgos, desde equivocaciones incidentales hasta errores que pudieron dificultar seriamente la marcha del proceso, como por ejemplo al inicio de la implantación del sistema en el área de emergencia, hubo pacientes que fueron atendidos y no se pudo hacer los descargos respectivos de los procedimientos médicos y de sus respectivos insumos, pudiendo ocasionar pérdidas económicas cuantiosas para esta casa de salud; nada más útil ante ello, que mantener los

canales departicipación ya mencionados, y usarlos para la autocrítica y para transparentar con humildad y franquezatanto los éxitos, como las dificultades y los errores.

4.5.2 LA RESISTENCIA AL CAMBIO

El grupo técnico multidisciplinario del hospital, al gestionar la resistencia, se ocupó de cuatro dimensiones del cambio: personal,interpersonal, gerencial y organizacional.

Se practicó que “enseñar” a aprender y a creer en los desafíos, y que las personas son capaces de hacer grandes cosas cuando piensan en grandes cosas. Es decir, “somoslo que pensamos que somos”. La clave de las técnicas que se utilicen para desencadenar el proceso estuvo en cuán exitosas sean en convocar a un pensamiento “común” de un nuevo hospital.

El lograr hacer pensar en todo el personal hospitalario el tener un mismo sentir, un mismo objetivo institucional fue determinante.

La permanente motivación en reuniones de trabajo con personal con el que se ejecutaba la implementación, hacerle ver los beneficios de disponer de un sistema automático que reduce el trabajo manual como por ejemplo recopilar un sin número de carpetas con historias clínicas abundantes y llevar a las consultas externas dio resultados positivos.

El Hospital Militar registra algunas oportunidades fallidas de implementaciones de un nuevo software hospitalario, no es raro encontrarse con que en oportunidades se ha decidido instalar un cambio, se ha hecho todo lo necesario, pero el cambio no funcionó, los síntomas que evidenciaron las oportunidades fallidas fueron:

- Mucha indiferencia por parte de la mayoría de personas en las diferentes áreas y

servicios.

- Mantener sobre todo el status quo.
- Las innovaciones, la tecnología, fueron ridiculizadas, como faltas de sentido e inteligencia.
- Existió un marcado esfuerzo por anular los efectos del cambio. Mantener los procesos antiguos.

Estos síntomas generados poralgunos motivos que a la postre son los que se identificó y se minimizó o eliminó para minimizar la resistenciaal cambio.

Cualquier intervención en un proceso, sea de orden técnico, organizacional o administrativo implica uncambio social, el pensar que una vez implantado el sistema hospitalario se iba a reducir personal administrativos sobre todo, empezó a causar problemas, lo que de manera inmediata se desvirtuó todos esos comentarios destructivos.

Por su parte, los individuos que forman parte de esta casa de salud resistieron a la implementación del sistema por:

- Ansiedades e inseguridades de permanecer o no en el trabajo:
- Temor de asumir riesgos con los cuales no están familiarizados, miedo a la tecnología.
- Temor a tornarse prescindible en su cargo por efecto del cambio.
- Temor de no ser capaz de manejar el sistema.
- Incapacidad o falta de disposición.

4.5.3 COMO INSTALAR CAMBIOS CUANDO HAY RESISTENCIA

Se realizó un diagnóstico en el hospital, de los puntos que tienden a producir resistencia y luego estructurarun proceso con sus actividades bien definidas. En el diagnóstico, se consideró:

- **¿Cuál es el tiempo que se tiene para completar el cambio?**

  180 días laborables.

- **¿Cuál es la intensidad de perturbación social y cultural que se creará?**

  Media alta, personal de enfermería, administrativo y médico sobre todo personal con más de 15 años en el hospital.

- **¿Quiénes serán afectados por el cambio?**

  Personal del área médica así como del área administrativa.

- **¿Quiénes serán los grupos o individuos que apoyarán o resistirán el cambio?**

  El escalón superior del HE-1 con la Dirección General y Dirección médica, el equipo técnico de implementación en apoyo decidido y constante.

  Los grupos que ofrecieron mayor resistencia al cambio fue principalmente el área administrativa especialmente el área financiera por ser el área en donde recae cualquier cambio de los procesos, procedimientos, servicio médicos que se traducen en impactos financieros y el departamento de Desarrollo Institucional por tener el impacto directo en los procesos institucionales.

- **¿Cuáles fueron los motivos para apoyar o resistir el cambio?**

  Los motivos por apoyar el cambio dentro de los más representativos fueron: el control integral del sistema tanto en el área médica y administrativa,

agendamiento automático, control de insumos médicos, facturación automática, aplicación del tarifario único de salud, mejora del servicio de salud, historias clínicas digitales, etc.

Una vez estudiado y diagnosticado elefecto del cambio, se practicó las siguientes medidas técnicas para gestionar la resistencia:

- **Transparencia**: Informar a toda la organización, sobre todo al personal de enfermería y médicos residentes y tratantes con el fin de reducir temores y ansiedades. Se detectó el grupo de mayor resistencia, especialmente médicos tratantes de mayor edad por temor a manejar un sistema informático, ante lo cual se dedicó mayor capacitación tipo personalizada y familiarización con el sistema.
- **Participación:** Se involucró a grupos de enfermería junto con personal de médicos y por servicio de hospitalización a fin de que inter actúen y vean los cambios y los beneficios en cada proceso, logrando disminuir la resistencia. Las personas tienden a dar apoyo a lo que han ayudado a crear.
- **Educación y entrenamiento**: Es imperativo entrenar a los afectados, ya que cualquier cambio significa olvidar hábitos y adquirir nuevos, aún más, los involucrados en el cambio deberán adquirir nuevas experiencias y olvidar experiencias pasadas, esto es lo que hemos definido como capacitación estratégica (aprender a aprender).

  Se incentivó a que el personal médico acuda a los videos de capacitación disponibles en la web (e-Learning hospitalario), al inicio de la implantación se

realizó una encuesta de quienes han revisado por lo menos una vez estos videos y el resultado fue mínimo, ante lo cual se dispuso a los jefes de piso que se realice una evaluación en base a los videos dando resultado positivo en el proceso.

- **Tiempo:** Se vio que la resistencia al cambio es mayor si se pretende hacer en un corto plazo y disminuye si el cambio es hecho en plazos mayores. En este proyecto fue un plazo adecuado de 180 días, ni muy corto ni tampoco muy largo.
- **Secuencia:** Los cambios se realizó en grupos pilotos basados en los turnos de trabajo y las guardias que maneja el personal médico, el grupo que entraba de turno mostraba mayor interés en la capacitación, el cambio fue exitoso, y existió un efecto de contagio donde el personal de enfermería empezó a dominar el sistema contagiando así al personal de médicos y residentes.

  Instalar los cambios por servicios o por pisos en el edificio de hospitalización, dio gran resultado, implantar de manera gradualen la torre de hospitalización por pisos, luego en las consultad externas fue una estrategia muy acertada.

4.6 PLANES DE PRUEBA

4.6.1 COORDINACIÓN Y EVALUACIÓN

Director Médico:	Dr. Roberto Navarrete
Coordinador Grupo:	Dr. Edwin Guerra
Coordinador ETI:	Ing. J Hugo Álvarez V.
Evaluación:	Jefes de servicios

4.6.2 TIPO DE PRUEBAS

USABILIDAD: Como ve el usuario el sistema

CARGA DE DATOS: Como funciona el sistema conmúltiples usuarios en la misma actividad.

DESEMPEÑO: Tiempos de respuesta

SEGURIDAD: Establecer las seguridades que el sistema debe mantener para garantizar la integridad de la información.

- **ADMISIÓN**
- **HOSPITALIZACIÓN**
  - **CIRUGIA VASCULAR**
  - **CARDIOLOGIA**
  - **CARDIOTORACICA**
  - **NEUMOLOGIA**
- **EMERGENCIA**

4.6.3 CALENDARIO DE PRUEBAS

AREA	FECHA	LUGAR
Admisión – Estadística	20 de marzo de 2013	Admisión y Estadística
Hospitalización	21 de marzo de 2013	Piso 8 Sala de Reuniones
Emergencia	22 de marzo de 2013	Emergencia
Quirófanos	26 de marzo de 2013	Tercer Piso
AREAS RELACIONADAS		
Farmacia	21-22-26 de marzo de 2013	Farmacia
Bodega	21-22-26 de marzo de 2013	Bodega de Insumos Médicos
Laboratorio	21-22-26 de marzo de 2013	Laboratorio
Imagen	21-22-26 de marzo de 2013	Imagen
Nutrición	21-22-26 de marzo de 2013	Nutrición
Facturación	21-22-26 de marzo de 2013	Finanzas

GRÁFICO 4.14: Calendario de Pruebas

4.6.4 PRUEBAS EN ADMISION Y ESTADISTICA

FECHA: 20 – MARZO – 2013

LUGAR: OFICINA DE ADMISIÓN Y ESTADISTICA

EQUIPOS 4 USUARIOS Y 4 TECNICOS

ACTIVIDADES:

- Internar a todos los pacientes hospitalizados en el piso 8
- Creación de un paciente por primera vez, asignar número HC
- Admitir un paciente ISSFA
- Admitir un paciente ISSFA familiar
- Admitir un paciente con referencia

OBJETIVO:

- Definir el funcionamiento del módulo de admisión
- Definir el proceso y documentarlo
- Comprobar la interacción con el área financiera
- Probar el sistema de ayuda en línea

4.6.5 PRUEBAS EN HOSPITALIZACIÓN

FECHA: 21 – MARZO – 2013

LUGAR: Sala de Sesiones del piso 8

PARTICIPANTES

- Dr. Juan Benalcázar Tratante Cirugía Vascular
- Dr. Juan Andrade Residente Cirugía Vascular
- Dr. Luis Jumbo Tratante Cardiología
- Dr. Jorge Vallejo Residente Cardiología
- Dr. Francisco Guerra Tratante Neumología
- Dr. Edwin Ayala Residente Neumología
- Dr. Jorge Pozo Tratante Cardiotorácica
- Dr. Andrés Bustamante Residente Cardiotorácica
- Lcda. Estela Dillon Jefe Enfermería
- Lcda. Wilma Vásquez Enfermera
- Lcda. Amparito Proaño Enfermera
- Ing. Rina Ortega Técnico SOFTCASE
- Ing. JakiroFeican Técnico SOFTCASE
- Ing. Geovanny Delgado Técnico de sistemas
- Ing. Eduardo Vásquez Técnico Procesos

EQUIPOS 17 USUARIOS Y 9 TECNICOS

ACTIVIDADES:

- Labores de enfermería para pacientes hospitalizados en el 8vo Piso
- Visita médica a pacientes hospitalizados en el 8vo. Piso
- Solicitud de exámenes, interconsultas, valoración cardiológica
- Elaboración de partes operatorios
- Elaborar prescripciones medicas
- Dar de alta a pacientes

OBJETIVO:

- Definir el funcionamiento del módulo
- Definir el proceso medico en hospitalización y documentarlo
- Comprobar la interacción con el área financiera
- Probar el sistema de ayuda en línea

4.6.6 PRUEBAS EN EMERGENCIA.

FECHA: 22 – MARZO – 2013

LUGAR: INSTALACIONES DEL SERVICIO DE EMERGENCIA

PARTICIPANTES:

Dr. William Montaluisa	Jefe Servicio
Dr. Fernando Chiriboga	Médico Tratante
Dr. Danilo Arauz	Médico Residente
Dr. Jorge Cortez	Médico Residente
Lcda. Alicia Arcos	Enfermera
Ing. Geovanny Delgado	Técnico de Sistemas
Ing. Francisco Olmedo	Softcase

Ing.JakiroFeican	Softcase
Ing. Rina Ortega	Softcase
Ing. Joel Paucar	Técnico Procesos

EQUIPOS 5 USUARIOS Y 9 TECNICOS

ACTIVIDADES:

- Internamiento por emergencia
- Labores de enfermería para pacientes en emergencia
- Solicitud de exámenes e interconsultas, prescripciones medicas
- Descargar medicamentos aplicados al paciente
- Dar de alta a pacientes
- Hospitalización paciente desde emergencia

OBJETIVO:

- Definir el funcionamiento del módulo de emergencia
- Definir el proceso medico en emergencia y documentarlo
- Comprobar la interacción con el área financiera
- Probar el sistema de ayuda en línea

4.6.7 PRUEBAS EN QUIRÓFANOS

FECHA: 26 – MARZO – 2013

LUGAR: INSTALACIONES DE QUIROFANOS 3er PISO

PARTICIPANTES:

Dr. Fernando Pérez	Jefe Servicio
Dr. de turno	Médico Tratante
Dr. de turno	Médico Residente

Dr. de turno	Médico Residente
Lcda. Nora Oña	Enfermera
Sr. Franklin Quintana	Farmacia Quirófanos
Ing. Geovanny Delgado	Técnico de Sistemas
Ing. Francisco Olmedo	Softcase
Ing. JakiroFeican	Softcase
Ing. Eduardo Vásquez	Técnico Procesos

EQUIPOS 6 USUARIOS Y 9 TECNICOS

ACTIVIDADES:

- Labores de enfermería para pacientes en quirófanos
- Descargar medicamentos aplicados al paciente
- Registro de actividades Post Operatorio
- Solicitud de exámenes
- Transferencia de pacientes al piso u otro servicio

OBJETIVO:

- Definir el funcionamiento del módulo de quirófanos
- Definir las actividades de post operatorio
- Comprobar la interacción con el área financiera
- Probar el sistema de ayuda en línea

4.6.8 PRUEBAS EN OTROS SERVICIOS

Farmacia:

Dra. Mónica Ramos	Jefe Farmacia
Dr. Julio Simbaña	Químico Farmacéutico

Personal de Turno	Técnico de farmacia
Ing. Francisco Olmedo	SOFTCASE
Ing. Eduardo García	Técnico de sistemas
Ing. Viviana Santacruz	Técnico Procesos

Bodega:

Mayo. Franklin Sánchez	Jefe IE de Bienes
SP. Walter Saavedra	Técnico de Bodega
Sgop. Luis Imbaquingo	Técnico de Bodega
SP. Luis Landeta	Técnico de Bodega
SP. Natalia León	Técnico de Bodega
Sgop. Esparza	Técnico de sistemas

Laboratorio:

Dra. Raquel Ubidia	Jefe laboratorio
Lcda. Verónica Castillo	Técnico de Laboratorio
Sgop. Darwin Dávila	Técnico de sistemas

Imagen

Dr. Gustavo Ramos	Jefe del Servicio
Sgop. Darwin Quishpe	Técnico Imagen
Sgop. Luis Cando	Técnico Imagen
Sra. Lourdes Pinto	Técnico Imagen

Nutrición:

Dra. Piedad Arellano	Nutricionista - Dietista
Sra. Martha Albán	Auxiliar de Alimentación

Ing. Rolando Proaño	Técnico de sistemas
Ing. Adriana Coronel	Técnico Procesos

Finanzas:

Dra. Adriana Heredia	Contabilidad
Ing. Guillermo Mejía	Tesorería
Ing. Leticia Moreno	Crédito y Cobranza
Sra. Yolanda Valencia	Cajas
Ing. David Nacimba	Técnico de sistemas
Ing. Joel Paucar	Técnico Procesos

4.7 CRONOLOGÍA DEL PROYECTO

Por disposición del Ministerio de Salud Pública todas las casas de salud a nivel nacional pasan a formar parte de la Red Pública Integral de Salud (RPIS), es así que a partir de Julio del 2012 el Hospital de Especialidades de FFAA ingresa a la RPIS como una casa de salud de nivel 3.

Posteriormente el Comando Conjunto dispone al HE-1 implemente un Sistema Informático de Gestión Hospitalario donado al Ministerio de Defensa Nacional, es así que en esta casa de salud a través de un proceso de lista corta se ejecuta el contrato **No. 2012-130-HE-1-ASEJ,** e inicia en el mes de septiembre del 2012 su implantación.

Para marzo del 2013 inician las primeras pruebas de sistema y es por el servicio de emergencia así como por el área de hospitalización que arranca este proyecto iniciando de manera formal el 1 de mayo del 2013, continuando por el servicio de laboratorios y finalizando para el mes de junio integrando el sistema en el servicio de consulta externa, como se indica en el gráfico: 4.14.

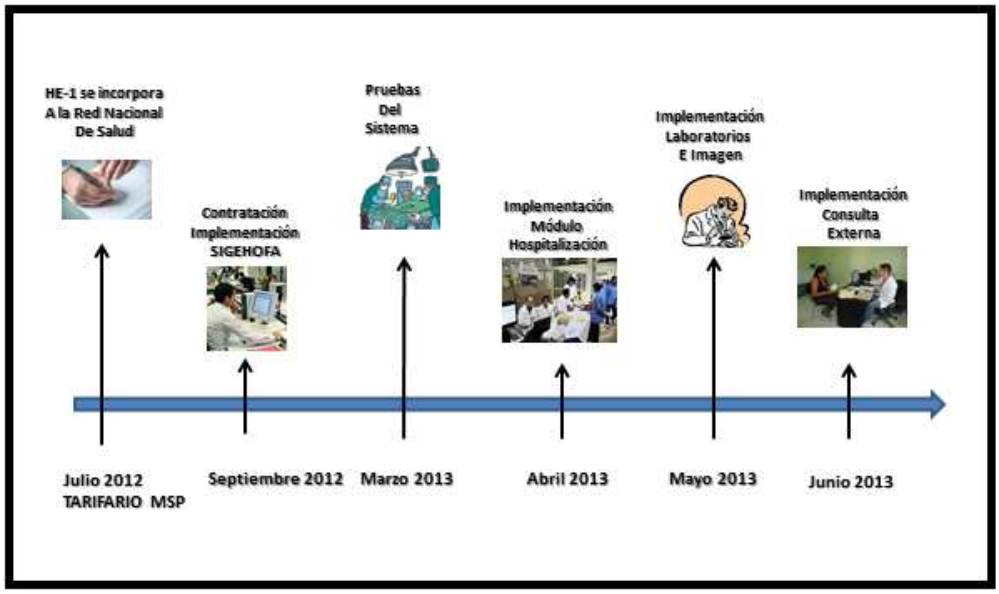


Gráfico: 4.14: Cronología del proyecto

En el gráfico 4.15, se muestra el desarrollo de la implementación del Sistema Informático de Gestión Hospitalario

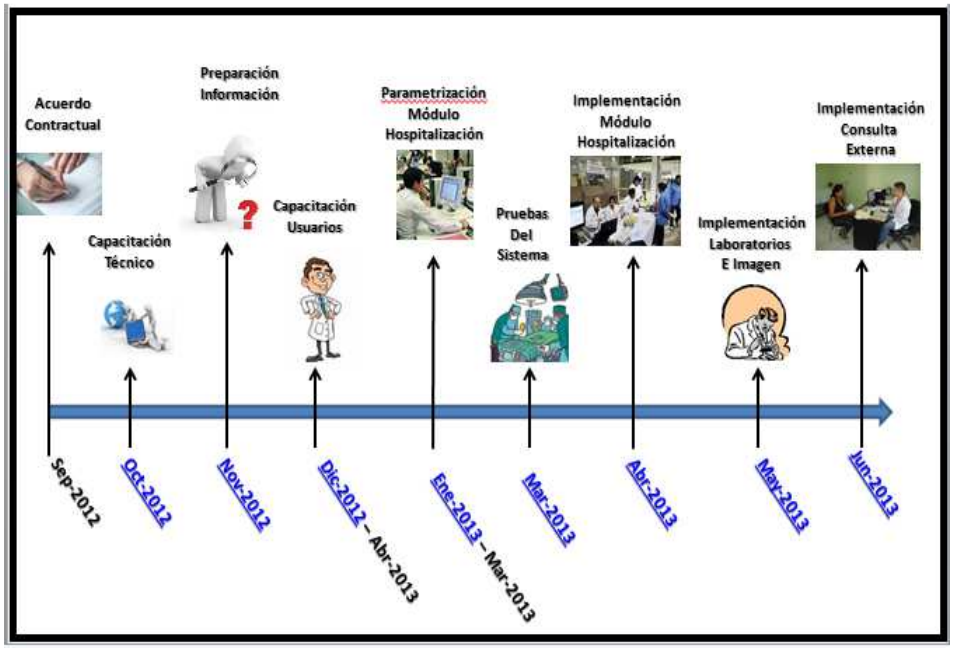


Gráfico 4.15: Proceso de implementación

4.8 FACTORES DE ÉXITO DEL PROYECTO

- El apoyo incondicional del Comando Conjunto de FFAA y principalmente la Dirección General de esta casa de salud fue determinante para tener éxito en la Implantación de un nuevo Sistema de Gestión Hospitalario.

- Equipo técnico multidisciplinario conformado por personal altamente capacitado como el del Director médico, Jefe del departamento de Tecnología de la Información y Comunicaciones del HE-1, personal asignado de las tres ramas de FFAA, todo el personal de enfermeras, médicos, así como también técnicos de la empresa propietaria del software fue el pilar fundamental para lograr el cambio hospitalario.

- El Software robusto, confiable y amigable permitió que el personal médico y administrativo se adapte de manera rápida.
- La infraestructura de red alcanzada para la implantación del sistema también fue otro factor de éxito, pues sin este soporte técnico no se hubiera podido implantar y estabilizar el Sistema Hospitalario.

- La Empresa donadora del software a través de su transparencia compromiso y espíritu nacionalista aportó también de manera importante para el éxito del proyecto.

C A P Í T U L O V:

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Implementación de la Red Segura

- El Ministerio de Defensa Nacional en el mes de marzo del 2012, dispone al Hospital de Especialidades de FFAA a través del COMACO la implementación del Sistema Informático de Gestión Hospitalaria para Fuerzas Armadas, ante este hecho el hospital en lo que respecta a la red existente se encontraba en la siguiente situación:

  La infraestructura de la red hospitalaria no se encontraba en condiciones para brindar integridad, confiabilidad y disponibilidad para cualquier aplicativo sobre esta red. El Back bone vertical en el edificio de hospitalización, era únicamente de Cu, limitando así la capacidad de comunicaciones en la trasmisión de datos a una velocidad máxima de 1 Gbps, no se disponía de racks de comunicaciones por piso, se encontró un crecimiento desordenado de la red de datos y un parque de computadores por cada proyecto de manera individual, sin un enfoque global.

- Durante este proyecto el Hospital de Especialidades de FFAA ha mejorado la infraestructura de red abriendo ventanas para la nueva tecnología hospitalaria como la telemedicina, Sistema radiológico en red, Imagen, sistema informático de gestión hospitalaria integral, quirófanos inteligentes, obteniendo de esta infraestructura de red: interoperabilidad, convergencia, escalabilidad, alta disponibilidad, seguridad y movilidad.

- Se implementó un nuevo data center bajo las normas y estándares que rige la tecnología, brindando una adecuada instalación con control de accesos, sistema de climatización, sistema de energía estabilizada.
- Este trabajo plantea una política de seguridad para una red segura, basada en la norma ISO 17799, esta política define el alcance de la seguridad de la red, la importancia que conlleva una red segura en una casa de salud, y define algunas disposiciones generales que son de gran valía a fin de garantizar conectividad, estabilidad y seguridad en toda la infraestructura de la red hospitalaria, esta norma permitió tener una guía, un marco referencial ampliando la visión y considerar otros aspectos para ir estructurando y tener una red hospitalaria segura mediante:

    - Un comité encargado de la gestión para la seguridad de la red con responsabilidades definidas.
    - Define claramente responsabilidades del oficial de seguridad de la red, dueño de datos, administradores de base de datos así como de la red, usuario final.
    - Se estableció controles para la clasificación de activos de la red, se estableció políticas para la selección de personal técnico.
    - Controles respecto a la seguridad física y del entorno, existe controles biométricos para el acceso a los data center, equipos activos de red en cuartos de comunicaciones por piso, bajo normas y estándares convencionales, suministro de energía estabilizada para toda la red, sistema de cableado estructurado categoría 6A. Controles acceso entre otros.

Implantación del Sistema de Gestión Hospitalario

No existía un Sistema de Gestión Hospitalario integrado, que permita un control tanto en la administración de salud así como en la administración logística y financiera, no se aplicaba las disposiciones emitidas por el Ministerio de Salud Pública como aplicación del tarifario único de salud, así como también la facturación de manera automática a los pacientes, esto hizo que el Hospital de Especialidades de FFAA implemente un nuevo sistema, actualmente esta casa de salud ya cuenta con el sistema integrado de gestión hospitalario, lo que ha permitido los siguientes beneficios:

a. El HE-1 aplica el tarifario único de salud dispuesto por el Ministerio de Salud Pública.

b. La facturación de los servicios prestados se hace de manera automática.

c. Un sistema de agendamiento por número de consultorio independiente del nombre del especialista.

d. El paciente puede ser atendido en más de una especialidad en consulta externa el mismo día si así lo amerita, (esto en función de la disponibilidad de los médicos).

e. La historia clínica de cada paciente estaba disponible en carpetas, las mismas que eran almacenadas en sus respectivas bodegas a donde el auxiliar de enfermería acudía de manera diaria según los turnos y las especialidades a retirar a fin de dar el servicio médico a los pacientes, este proceso causaba deterioro de las historias clínica, pérdidas, hoy se dispone la información de cada paciente en el sistema informático línea.

f. La asignación de turnos para los diferentes pedidos de exámenes de laboratorio, imagen era otro caos permanente, pues se lo hacía de manera manual y existía gran afluencia de pacientes quienes recibían turnos hasta para un mes para sus exámenes hoy en día se hace el pedido y los resultados en el sistema informático en línea.

g. El médico tratante puede dar citas médicas subsecuentes a los pacientes que requieren el control de manera que ya no deben sacar un turno en las cajas, este turno subsecuente puede ser asignado para la fecha que el médico tratante requiere hacer el nuevo control o chequeo médico.

h. El control de insumos médicos, medicamentos aplicados, información financiera, se lo realizaba de manera independiente no existía una información cruzada entre el procedimiento médico y el registro de bodegas, el sistema informático instalado es integral y permite un cierre de bodega de manera exacta por cada insumo médico, esto es trascendental en el hospital.

i. El sistema de Gestión Hospitalario permite llevar un control de servicios prestados, obtener estadísticas generales de los pacientes, obtener datos epidemiológicos, detallar el costo de la atención prestada a cada paciente y sobre todo llevar un estricto expediente clínico electrónico el mismo que es controlado por auditoría médica.

j. La organización alcanzada no tiene nada que ver con la situación anterior así como el ahorro de tiempo, papel, gestión personal y horas de trabajo.

Gestión del Cambio

La identificación de los grupos que ofrecieron mayor resistencia al cambio como son el área administrativa y financiera así como el personal médico de mayor edad, permitió que se realice un seguimiento del proceso del cambio de manera más cercana, dando más atención y capacitación personalizada.

La forma de implantar el nuevo sistema de manera paulatina y mantener paralelo el sistema antiguo permitió tener confianza al personal médico (Enfermeras y médicos).

La gestión del cambio permitió implantar el sistema hospitalario minimizando al máximo los impactos en las áreas como: médica, logística, financiera y administrativa, evitando así consecuencias que pudieron poner en riesgo los objetivos institucionales.

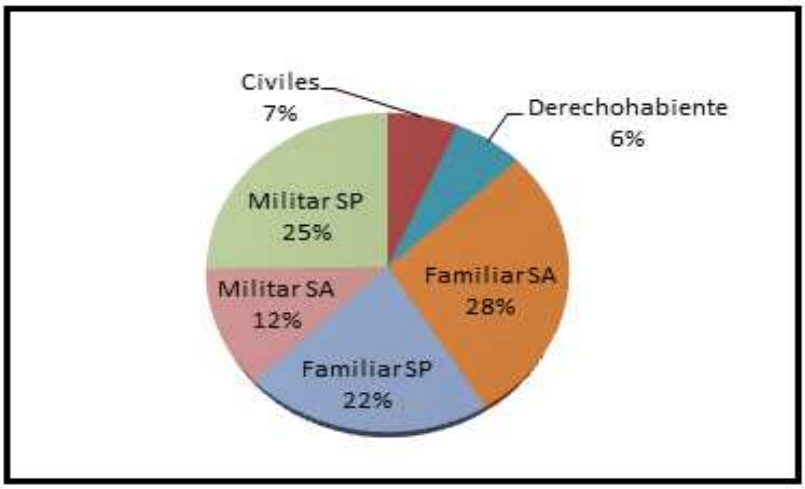
El nuevo sistema de gestión hospitalario generó un gran impacto institucional, el manejo de la gestión del cambio en base a la transparencia del proceso, la información y socialización permitió resultados positivos como podemos plasmar con las siguientes estadísticas:

Los datos se obtienen sobre la base del "Manual de Normas y Procedimientos del Sistema de Información en Salud de Fuerzas Armadas, SISFA"

Atenciones por tipo de usuario

Durante el año 2013 solicitaron atención un total de 54918 usuarios en los diferentes Servicios Médicos de esta Casa de Salud. En el gráfico No. 5.1, vemos la distribución de los pacientes que solicitaron atención por tipo y su tendencia. Los usuarios ISSFA representan el 93 % del total, siendo: los familiares del militar en servicio activo y pasivo quienes demandan con mayor frecuencia atención (50%), seguido de los

militares en servicio pasivo (22%), activo (12%) y derechohabientes (6%). Los usuarios civiles representan el 7 %.

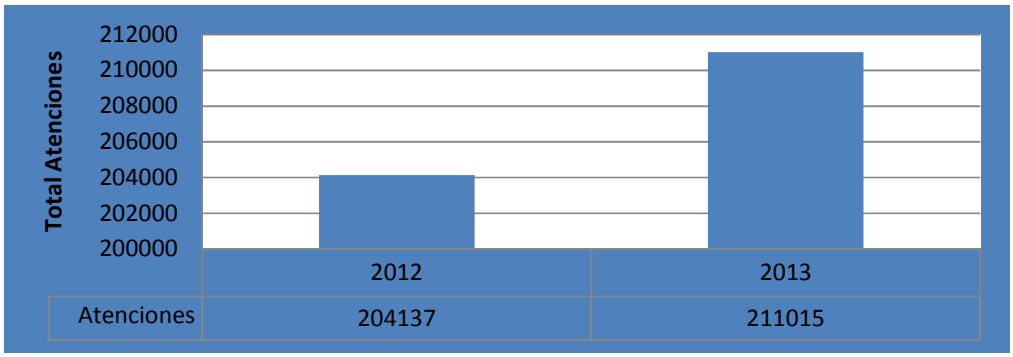


Fuente: Sistema de Gestión Hospitalario
Realizado: Ing. Juan Dillon

Grafico 5.1: Porcentaje de pacientes que solicitaron atenciónen el HE-1-Año 2013

Atención en Consulta Externa

Durante el año 2013, el hospital contó con 35 especialidades y 98 consultorios para brindar atención en consulta externa. Los consultorios fueron utilizados un promedio de 4 horas diarias. Se programaron un total de 248170 consultas, de las cuales se realizaron un total de 211015 consultas, que representa el 85 % de lo programado. Diariamente se atendió un promedio de 844 usuarios, de los cuales el 29 % fueron consultas de primera vez. Se atendió un promedio de 2.89 pacientes por cada hora médico programada que al comparar con el estándar que es de 4 pacientes hora médico, encontramos que es aceptable, siendo la principal causa del incumplimiento el ausentismo de los usuarios, que se situó en el 15 %, como se muestra en el gráfico 5.2.



Fuente: Sistema de Gestión Hospitalario(Dillon, 2013)
Realizado: Ing. Juan Dillon

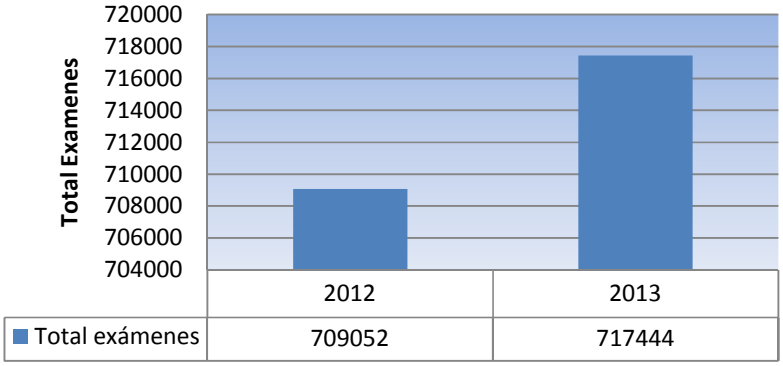
Gráfico 5.2: Total de Atenciones en Consulta ExternaHE-1-Año 2012-2013

Para el año 2013 existe un incremento del 3.37 % al relacionar el total de atenciones con el año 2012. Se identifica como causa principal el incremento de la oferta en horas médicas a través de la implementación de la Agenda Médica del Sistema de Gestión Hospitalario. Además existe una racionalización del turno subsecuente por cuanto es asignado por el médico tratante conforme a la necesidad de atención del paciente.

Exámenes de laboratorio

Durante el año 2013, se realizaron un total de 717444 exámenes de laboratorio, con un promedio diario 2836 exámenes. Del total de exámenes el 57 % fueron solicitados por consulta externa, con un promedio de 1.93 exámenes por cada atención en consulta externa; el 26% son solicitados por hospitalización, con un promedio de 19 exámenes por egreso; el 17 % son solicitados por emergencia, con un promedio de 3 exámenes por cada paciente atendido.

En el gráfico 5.3 se presenta el total de exámenes de laboratorio del año 2012 y 2013, existiendo un incremento del 11 %. Mejorando sobre todo el pedido y entrega de resultados de manera automática a través del Software de Gestión Hospitalario.



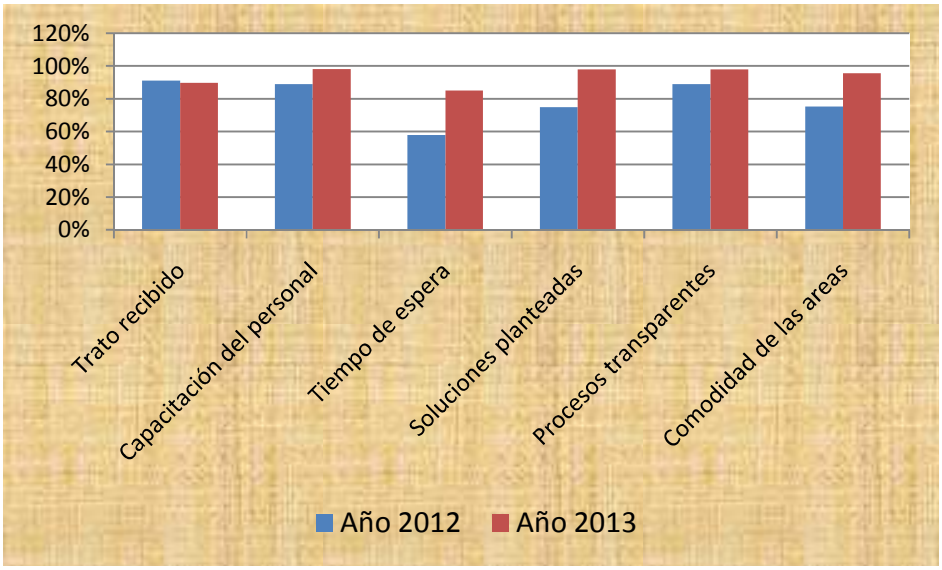
Fuente: Sistema de Gestión Hospitalario
Realizado: Ing. Juan Dillon

Gráfico 5.3: Total de Exámenes en LaboratorioHE-1-Año 2012-2013

Satisfacción de Usuarios

Durante el mes de octubre se realiza un total de 155 encuestas a los usuarios que utilizan los servicios de consulta externa, obteniendo como resultado una satisfacción del 98 %, calificando la atención como muy buena (78 %) y buena (20 %). Al comparar con el año 2012, se evidencia una mejora en el tiempo de espera para facturar los turnos, exámenes y procedimientos, manifestando el 85 % de los usuarios que se demoran entre 5 y 30 minutos, calificándole de adecuado; esto se logró con la implementación del nuevo Sistema de Gestión Hospitalario, por cuanto el 90 % de los usuarios ya no se acercan a las cajas a cancelar los exámenes y procedimientos.

Además, los usuarios encuentran satisfacción con la infraestructura (98 %), el acceso principal (98 %), la comodidad de las salas de espera (90 %) y la limpieza de los baños (97 %), siendo el resultado de la readecuación que se realizó en el Edificio de Consulta Externa, como se muestra en la figura 5.4



Fuente: Encuesta Consulta Año 2013
Realizado: Ing. Juan Dillon

Gráfico 5.4: Satisfacción de los usuarios

5.2 RECOMENDACIONES

Implementación de la Red Segura

- La infraestructura de red alcanzada con este proyecto es muy importante para el hospital y con el apoyo permanente y comprometido de la Dirección General, se requiere la disponibilidad de profesionales capacitados que cumplan con las funciones de administradores de redes y base de datos, que tengan nombramiento en esta casa de salud, ya que al momento no existe este personal con estabilidad laboral y se vuelve en una debilidad que podría comprometer la operatividad de la red segura.

- Apoyar al comité conformado para la seguridad de la red, a fin de que se cumplan sus funciones y responsabilidades establecidas en este trabajo y puedan ejecutar el ciclo de mejora continua, a fin de brindar integridad, confiabilidad y disponibilidad de la información que sea transmitida por la infraestructura de red hospitalaria.

- Obtener una autorización institucional de la Política de Seguridad para la Red Segura, planteada en este proyecto a fin de cumplir los objetivos institucionales.

Implementación del Sistema de Gestión Hospitalario

- Para el mantenimiento del software se debe mantener el soporte técnico por lo menos durante un año a partir de su implantación con personal de la empresa dueña del sistema de gestión hospitalario.

- Desarrollar nuevos módulos de acuerdo a las nuevas existencias que se vayan presentando como son el intercambio de información en la Red Pública Integral de Salud, así como implementar un servicio de imagen en red de alta resolución, un módulo de gestión de calidad con encuestas de satisfacción con firma electrónica, abrir la ventana de la telemedicina y lograr ser un hospital docente que sea referente a nivel nacional.

Gestión del Cambio

- Se debe identificar en que niveles de la organización existirá más resistencia al cambio a fin de desplegar un mayor esfuerzo y reducir al máximo los impactos en esas áreas evitando así consecuencias que pudieran poner en riesgo el cambio y los objetivos institucionales.
- Mantener una capacitación permanente sobre la tecnología alcanzada en esta casa de salud sobre todo en el nuevo sistema de gestión hospitalario, a fin de que el personal médico como administrativo no desarrolle el estatus quo y tenga una visión de mejora continua en todos sus procesos.

- A través de un proceso estratégico, el equipo directivo puede elaborar planes y metas específicas para mantener la ruta en la “gestión del cambio”; ante las eventualidades y los imprevistos, hacer la evaluación de riesgos y poder evaluar y señalar los resultados para ir retroalimentando y modulando el ritmo del proceso es sumamente importante. Cerrar brechas o avanzar hacia la realización

de la imagen deseada implica decisiones estratégicas, que modifican en alguna forma la naturaleza del hospital.

Constituyen oportunidades para el cambio, situaciones como la implementación de un nuevo sistema informático de gestión hospitalario, un nuevo servicio, inter consultas médicas, la ampliación de la cobertura, la adopción de nuevas formas de atención en los servicios de emergencia por ejemplo, son nuevos retos planteados.

Estas decisiones pueden plantear tareas de envergadura al hospital, pues repercuten sobre muchas de las funciones y rutinas anteriores; por ejemplo, las relaciones con procesos diferentes, nuevas prácticas, la asignación de recursos, las habilidades y conocimientos de trabajadores de salud, administrativos y técnicos.

El desafío impostergable de este tiempo es avanzar a la excelencia institucional en salud pública;

Esperar avanzar sistemática y consistentemente a establecimientos hospitalarios de clase mundial hacia fines de la presente década.

BIBLIOGRAFÍA

2008, A. C. (10 de Agosto de 2008). CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR 2008. *PRESTACIONES MÉDICAS*. Manta, Portoviejo, Ecuador.

Constituyente, A. (2008). LEY ORGÁNICA. *LEY ORGÁNICA DEL SISTEMA NACIONAL DE SALUD*.

HE-1, D. d. (1 de AGOSTO de 2012). Plan Esyratégico 2012-2016 del HE-1. *Modelo de Gestión* . QUITO, Pichincha, Ecuador.

http://monografias.com. (s.f.). Obtenido de http://monografias.com/trabajos42/iso-informatica/iso-informatica2.shtml.

http://www.isotools.org. (s.f.). Obtenido de http://www.isotools.org/tag/iso-27001.

NTC-ISO/IEC 17799. (s.f.). *Norma Técnica Colombiana NTC-ISO/IEC 17799 código de buenas prácticas para la Gestión de la Seguridad de la Información*. Bogota, Colombia. http://www.guiadelacalidad.com/modelo-efqm/gestion-del-cambio.

Tesis “Seguridad Informática: sus implicaciones e implementación” Copyright Cristian F. Borghello2001 webmaster@cfbsoft.com.ar , www.cfbsoft.com.ar.