Análisis de Seguridad Informática

Hospital General “Madre Teresa de Calcuta” HG-MTC

Autor: Oniel S. Gutiérrez Reyes

Universidad Tecnológica De La Habana “José Antonio Echeverría”
Facultad De Ingeniería Informática

CUJAE
La Habana, Cuba
2018

ÍNDICE

1.1. Generales de la institución 3
1.2. Objetivos del Sistema Informático 3
1.3. Componentes de Hardware 4
1.4. Componentes de Software 5
1.5. Conectividad externa 5
1.6. Soporte de energía 6
1.7. Recursos Humanos 6
2. DIAGRAMA FÍSICO 7
3. DIAGRAMA LÓGICO 8
3.1. Representación lógica del servicio de imagenología médica en tiempo real 8
3.2. Representación lógica del acceso remoto controlado a los equipos médicos para la recogidade datos 8
3.3. Representación lógica del acceso a información de camas disponibles. 8
4. INVENTARIO DE RECURSOS DEL SISTEMA INFORMATICO 9
5. CÁLCULO DE LA DISPONIBILIDAD 10

5.1 Calcular la Cantidad de Fallos (CF) y Tiempo de Fallos de Servicios (TFS) para cada elemento 10
5.2 Cálculo horas de explotación de cada componente 11
5.3 Cálculo para la disponibilidad del servicio en cuestión 11
Segundo Diagrama - Acceso remoto controlado a los equipos médicos para la recogidade datos 11
6. ANÁLISIS DE LOS COMPONENTES QUE MÁS HAN FALLADO 12
6.1. Analizar los riesgos que conlleva. Clasificación en Importancia y Valor 13
6.2. Evaluación de violaciones, riesgos que conllevan y las políticas para mitigarlos 14
6.3. Políticas y medidas para mitigarlos 16
7. CÓDIGO ÉTICA DEL HG-MTC 17

Hospital General “Madre Teresa de Calcuta” HG-MTC, ubicado en la zona urbana central de la Ciudad. Cuenta con 650 camas de ingreso y todas las especialidades clínicas, brinda servicios a unos 300 mil habitantes de la ciudad y otros 25 mil de áreas rurales. Es la institución principal del sistema de salud de la región donde existen además otros 3 hospitales especializados en oncología, pediatría y maternidad. Otras 50 clínicas y consultorios que tributan al HG-MTC pacientes a remisión según las emergencias o enfermedades detectadas. El Hospital cuenta con un área docente de 6 aulas, un plenario y 2 laboratorios de informática donde además de la docencia se permite el tiempo de máquina para servicios de navegación, correo y edición de materiales. También tiene un centro de información con materiales impresos y digitales. Alberga entre sus especialistas al grupo nacional de procesamiento de imágenes médicas y al de cirugía endoscópica de alta precisión.

EL hospital cuenta con equipos médicos altamente informatizados para imagenología, radioterapia, etc. conectados a la red de datos de la institución.

El HG-MTC cuenta con un nodo central de telecomunicaciones y tres subnodos uno en el área clínica, uno en el área de consultas y otro en el área docente, todos están climatizados con sistemas industriales y están conectados al sistema de emergencia eléctrica de respaldo. El backbone del cableado es a FO MM, entre los subnodos y el nodo central.

Cada subnodo posee como promedio 3 servidores de hardware de distintos fabricantes y prestaciones:

El subnodo de consultas posee unas 25 PC’s como estaciones de trabajo de las consultas y hay otros 30 equipos médicos conectados a la red de datos, todos mediante una red UTP Cat 5e.

En el subnodo del área clínica hay un cableado UTPCat 5e diferenciado para los equipos médicos del cableado de las 20 estaciones de trabajo para el personal médico. Hay un bloque de alojamiento a pacientes especiales (10 posiciones) que tienen la posibilidad de navegar por Internet cuando llevan sus equipos propios.

El subnodo del área docente atiende los laboratorios, las aulas y el plenario con facilidades de trabajo colaborativo, práctica docente y acceso a Internet, pudiendo transmitirse video y audio en tiempo real desde las salas de operaciones del área clínica a estos espacios docentes mediante un enlace tipo Internet2 (I2) a 622 Mbps y con IPv6.

En la red del HG-MTC se ha interconectado el nodo Central a los subnodos de modo

redundante 1:2 mediante enlaces de FO MM y switches de nivel 2 administrables y configurables de modo remoto.

Cada subnodo posee un router CISCO de 1 puerta WAN 2 a Mbps sobre FO y 2 puertas LAN 100/1000 Ethernet RJ45. El nodo Central cuenta con 2 Router CISCO cada uno con 2 puertas WAN a 2 Mbps FO y 2 puertas Gigabit Ethernet, para implementar junto a dos firewall por hardware una zona segura (desmilitarizada, DMZ) donde se ubican los servicios externos y un servidor RAS por hardware de 64 puertas conmutadas. Hacia dentro de la DMZ hay una copia de los servidores que garantizan los servicios centralizados del campus (RAS, DNS en los dos niveles, acceso a internet, etc.).

El nodo central posee un espejo de la información en los servidores de cada subnodo. Las salvas de datos de todos los sistemas se realizan instantáneamente según volumen de las transacciones de los servicios. De no haber eventos de modo obligado ocurren cada 6 horas.

El HG-MTC ha contratado los servicios de un DATACENTER externo al hospital donde se guarda de modo seguro toda la información relacionada con las historias clínicas y la actividad de los pacientes.

Sistemas Operativos
Se emplea como SO generalizado en las estaciones de trabajo el Windows, (XP SP3, Win7 R2) y en los subnodos se ejecutan versiones de Suse Linux.
Los equipos médicos poseen sus SO personalizados, pero todos basados en WinCE.

El segmento de red I2 posee sistema Operativo Windows 2008 SERVER con varias aplicaciones desarrolladas sobre Java para realizar Streaming de audio y video.

Aplicaciones

Se emplean aplicaciones de Software de cualquier tipo por los pacientes de la sala con navegación, internamente los equipos del personal médico y hospital emplean el MS Office aunque están migrando paulatinamente a Open Office v 10.2.

La gestión de usuarios la realiza el nodo central como parte de un dominio general hgmtc.sld.cu.

Los servicios de conectividad exterior del HG-MTC poseen la siguiente estructura:

EL HG-MTC recibe la energía eléctrica desde la Red Nacional a través de dos subestaciones (circuitos) independientes de 13 Kv, se cuenta con un grupo electrógeno de respaldo completo para el área de cirugía, hospitalización y emergencias, y de modo parcial (sin clima) para las restantes áreas.

El nodo central y cada subnodo poseen UPS que garantizan 2 horas de respaldo a los servicios tele informáticos por 8 horas. Los equipos pueden satisfactoriamente trabajar sin clima 2 horas posteriores a la falla eléctrica.

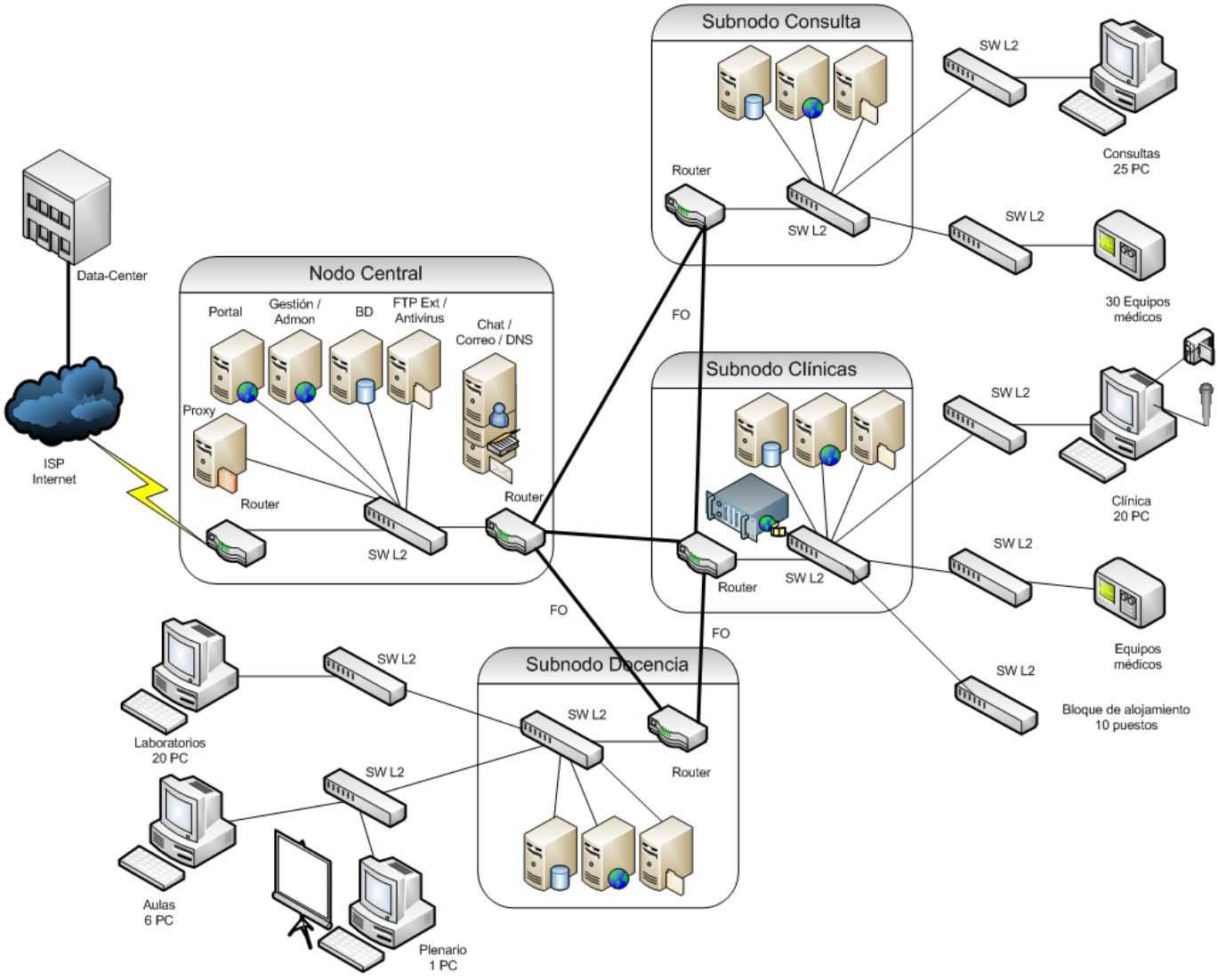
EL HG-MTC cuenta con un Departamento de Equipos y Tecnologías que atiende todos los

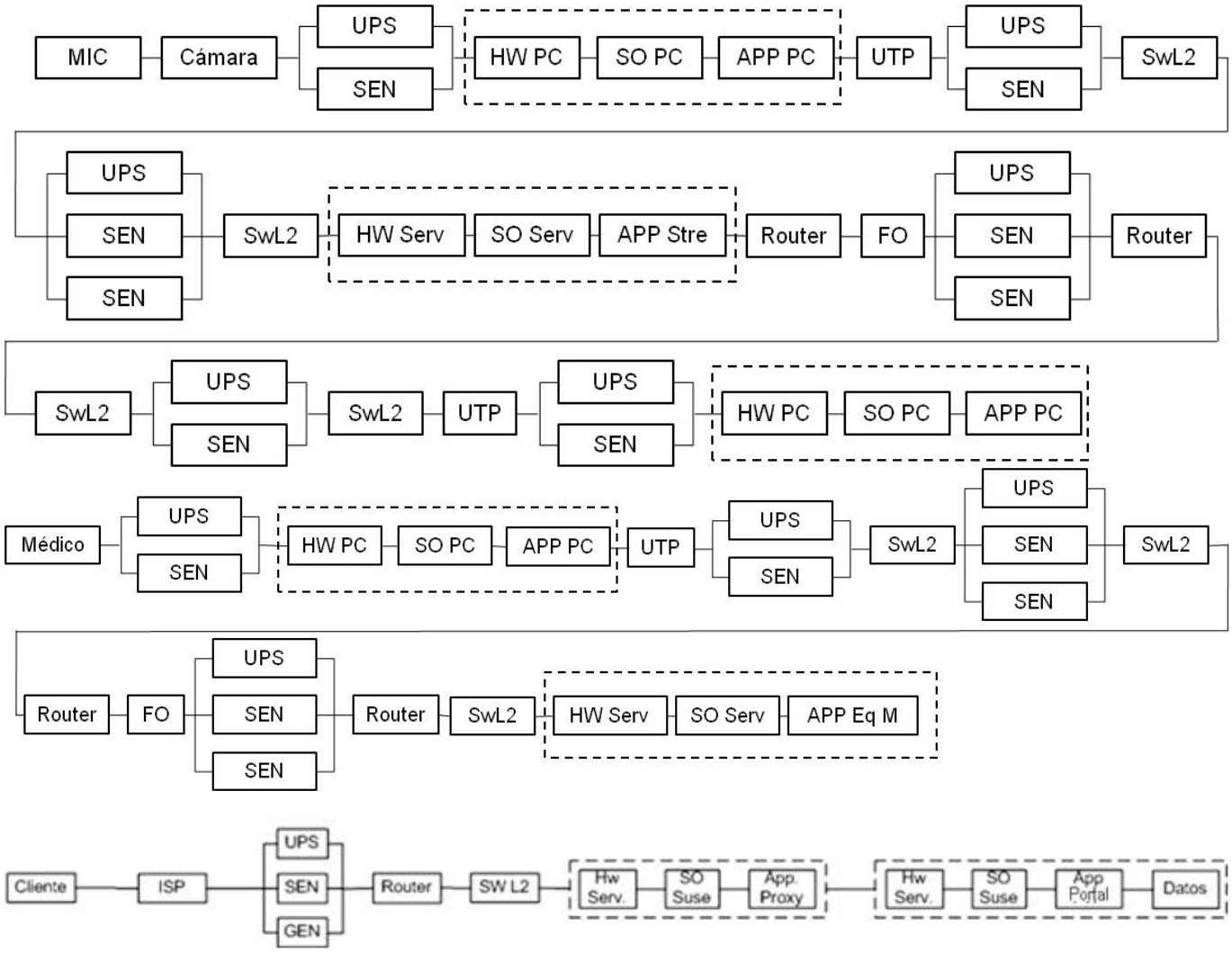
equipos médicos y además la red de datos y computadoras del centro, además del jefe y del jefe técnico hay un responsable de seguridad de datos y 1 Ing. en tele, hay además otros 6 técnicos especializados por tipo de servicios según los equipos, uno de ellos en computadoras.

En el departamento de auditoría hay un auditor especializado en seguridad informática de los sistemas contables-financieros y en Dpto. legal hay un especialista en legalidad informática.

Siempre hay un administrador o técnico de guardia, las 24 horas x 365 días en el nodo central de la red.

Representación física de la red donde se explota este SI





No.	COMPONENTES DEL SISTEMA INFORMÁTICO		CANT	CF	TFS (hrs)	DF	Costo
1	HARDWARE	Router CISCO puertas WAN	5	2	8	Lineal	2100
2		Switch L2	11	3	24	Lineal	759,00
3		Servidor	15	3	12	Cuadrática	4200,00
4		PC	112	16	120	Cuadrática	1200,00
5		Equipos Médicos	30	0	0	0	0,00
6		UPS	4	15	50	Lineal	9200,00
7		Generador	1	0	0	0	0,00
8		Sistema Eléctrico Nacional	1	300	120	Constante	25000/mes
9		Streaming Audio y Video	27	16	120	Lineal	1200,00

10		Enlace Internet2 (I2)		27	12	26	Constante	120,00
11		Cableado UTP Cat 5e		500 m	12	26	Constante	120,00
12		Fibra Óptica		400 m	2	12	Constante	3500,0
13	SOFTWARE SERVIDOR	SO	Suse Linux	15	5	48	Constante	1200,00
14		APP	vsftpd, firefox, Squid, Outlook, MySQL, Bind9, Apache, Kaspersky		10	38	Constante	150,00
15	SOFTWARE PC	SO	Windows	112	3	30	Lineal	225
16		APP	MS Office		18	122	Lineal	1200,00
17	SOFTWARE EQUIPOS MÉDICOS	SO	WinCE	30	3	30	Lineal	225
18		APP	Imagenología, radioterapia, etc					
19	SOFTWARE STREAMING AUDIO Y VIDEO	SO	Windows 2008	27	3	30	Lineal	225
20		APP	Java Streaming		3	30	Lineal	225
21	RECURSOS HUMANOS	Jefe		1	45 días		Constante	500 $/mes
22		Jefe técnico		1	30 días		Constante	450 $/mes
23		Responsable de seguridad de datos		1	45 días		Constante	450 $/mes
24		Ingeniero en Telecomunicaciones		1	45 días		Constante	500 $/mes
25		Técnicos Especializados		6	30 días		Constante	450 $/mes
26		Auditor Especializado en Seguridad Informática		1	20 días		Constante	500 $/mes
27		Especialista en legalidad informática		1	25 días		Constante	500 $/mes
28		Administrador		1	30 días		Constante	500 $/mes

COMPONENTES DEL SISTEMA INFORMÁTICO		VOLUMEN
DATOS	Configuración FTP, Proxy, DNS, Router, Antivirus	23 Kb
	Imágenes médicas	50 Mb
	Datos del paciente, usuario	150 Kb
	Documentos científicos	2 Gb
OW	Plan de Seguridad Informática	400 Kb
	Código ética, Ley 60 y Ley 127	145 Kb
	Autorizo de explotación de la red	83 Kb
	Plan de contingencia, de evacuación	25 Kb

2017	Se proyecta al año		2018		2017	Se proyecta al año		2018	
Router	CF	TFS	CF	TFS	UPS	CF	TFS	CF	TFS
Lineal	y=2x+n	y=2x+n	y=2x	y=2*2+6	Lineal	y=3x+n	y=3x+n	y=3x+12	y=3x+47
CF=2	2=2*1+n	8=2*1+n	y=2*2	y=4+6	CF=15	15=3*1+n	50=3*1+n	y=3*2+12	y=3*2+47
TFS=8	0=n	6=n	y=4	y=10	TFS=50	12=n	47=n	y=18	y=53
C=5	y=2x	y=2x+6			C=4	y=3x+12	y=3x+47		

Servidor	CF	TFS	CF	TFS	Audio-Video	CF	TFS	CF	TFS
Cuadrática	$y=3x^2+n$	$y=3x^2+n$	$y=3x^2$	$y=3x^2+9$	Lineal	y=2x	y=2x	y=2x+14	y=2x+118
CF=3	3=3*1+n	12=3*1+n	$y=3*2^2$	$y=3*2^2+9$	CF=16	16=2*1+n	120=2*1+n	y=2*2+14	y=2*2+118
TFS=12	0=n	9=n	y=12	y=21	TFS=120	14=n	118=n	y=18	y=122
c=15	$y=3x^2$	$y=3x^2+9$			C=27	y=2x+14	y=2x+118		
Switch	CF	TFS	CF	TFS	UTP	CF	TFS	CF	TFS
Lineal	y=x+n	y=x+n	y=x+2	y=x+23	Constante	12	26	12	26
CF=3	3=1+n	24=1+n	y=2+2	y=2+23	CF=12				
TFS=24	2=n	23=n	y=4	y=25	TFS=26				
C=11	y=x+2	y=x+23			C=500				
PC	CF	TFS	CF	TFS	FO	CF	TFS	CF	TFS
Cuadrática	$y=x^2+n$	$y=x^2+n$	$y=x^2+15$	$y=x^2+119$	Constante	2	12	2	12
CF=16	16=1+n	120=1+n	$y=2^2+15$	$y=2^2+119$	CF=2				
TFS=120	15=n	119=n	y=19	y=123	TFS=12				
C=112	$y=x^2+15$	$y=x^2+119$			C=400				
SEN	CF	TFS	CF	TFS	**FO**	CF	TFS	CF	TFS
Constante	300	120	300	120	Constante	0	0	0	0
CF=300					CF=0				
TFS=120					TFS=0				
C=1					C=1				

UPS	53/4=13,25		SW	25/11=2,272		GEN	0		FO	0
	$D_{ups/u}=0,999$			$D_{sw/u}=0,998$			$D_{GEN}=1$			$D_{FO}=1$
Audio/Video	122/27=4,518		Router	10/5=2		SEN	120/1=120		FORMULAS	
	$D_{A-V/u}=0,986$			$D_{R/u}=0,999$			$D_{SEN/U}=0,986$		(I) TFS/CE	
									$D_{E/U}$= 8760 - (I) /8760	
PC	123/112=1,098		UTP	26/500=0,052		SERV	21/15=1,4		$0 < D_T < 1$	
	$D_{PC/u}=0,987$			$D_{UTP/u}=0,942$			$D_{SERV/U}=0,998$			

Distribución en Paralela		Distribución de 3 elementos	
$D_P=1 - [(1-D_{ups/u})(1-D_{SEN/U})]$		D_{3E}:	$X=1 - [(1-D_{ups/u})(1-D_{SEN/U})] =$ 0,999
Dp=1 - 0,000014			$Y=1- [(1-D_{GEN/U})(1-X)] = 1$
Dp=0,999		$D_{3E} = 1$	

Primer Diagrama - Servicio de imagenología médica en tiempo real						
$D_T = D_{ups/u} *(D_{P/U})^4 * (D_{PC/U})^2 * (D_{UTP/U})^2 * (D_{SW/U})^4 * (D_{3E/U})^2 * D_{SERV/U} * (D_{R/U})^2 * D_{FO}$						
$D_T=0,836$						
83,60%						
$D_T= (D_{P/U})^2 * (D_{PC/U}) * (D_{UTP/U}) * (D_{SW/U})^3 * (D_{3E/U})^2 * (D_{R/U})^2 * D_{FO} * D_{SERV/U}$						
$D_T=0,917$						
91,70%						
Tercer Diagrama - Acceso a información de camas disponibles.						
$D_T= (D_{3E/U}) * (D_{R/U}) * (D_{SW/U}) * (D_{SERV/U})^2$						
$D_T=0,993$						
99,30%						

No.	COMPONENTES DEL SISTEMA INFORMÁTICO			IMPORTANCIA	VALOR
1	SOFTWARE SERVIDOR	SO	Suse Linux	Alta	Bajo
2		APP	vsftpd	Baja	Bajo
3			Firefox	Media	Bajo
4			Squid	Media	Bajo
5			Outlook	Baja	Bajo
6			MySQL	Alta	Alto
7			Bind9	Alta	Alto
8			Apache	Alta	Alto
9			Kaspersky	Baja	Bajo
10	SOFTWARE PC	SO	Windows	Baja	Bajo
11		APP	MS Office	Media	Medio
12	SOFTWARE EQUIPOS MÉDICOS	SO	WinCE	Alta	Alto
13		APP	Imagenología, radioterapia, etc	Alta	Alto
14	SOFTWARE STREAMING AUDIO Y VIDEO	SO	Windows 2008	Alta	Alto
15		APP	Java Streaming	Alta	Alto
16	DATOS	Configuración FTP		Media	Medio
17		Configuración Proxy		Alta	Alto

18		Configuración DNS	Alta	Alto
19		Configuración Router,	Alta	Alto
20		Configuración Chat	Media	Medio
21		Configuración Antivirus	Baja	Bajo
22		Imágenes médicas	Alta	Alto
23		Datos del paciente, usuario	Alta	Alto
24		Documentos científicos	Baja	Bajo

Importancia				
Alta	1, 6, 7, 8		**12, 13, 14, 15, 17, 18, 19, 22, 23**	
Media	3, 4	11,16, 20		
Baja	2,5,9,10,21,24			**Valor**
	Bajo	Medio	Alto	

Cuadrante AA: Alta probabilidad y alto valor. Riesgos: **12, 13, 14, 15, 17, 18, 19, 22, 23**

Vulnerabilidad		**Riesgo**		**Valor**	**Importancia**
V1	Problemas de disponibilidad de Audio/Video.	R1	Dejar fuera de operaciones los servicios al personal médico	Baja	Alto
		R2	Se queda sin supervisión el Sistema.	Baja	Alto
V2	Problemas de disponibilidad del SEN.	R3	Deja fuera de servicio los equipos médicos.	Media	Alto
		R4	Fallas del SW de los equipos provocan inconsistencia, deterioros en las BD	Baja	Alto
V3	No existencia de respaldo UPS a la PC del Administrador	R5	No se realizan tareas de supervisión de la red.	Medio	Medio
		R6	No se pueden restablecer los servicios ante un incidente.	Alto	Medio
V4	Problemas de disponibilidad de la PC del administrador	R7	No se realizan tareas de supervisión de la red	Medio	Medio
		R8	No se pueden restablecer los servicios ante un incidente	Alto	Medio
V5	Conectividad	R9	Baja disponibilidad de acceso a los sistemas de los equipos.	Alto	Alto
Cualquier otra vulnerabilidad que influya en que el Administrador no pueda gestionar los equipos médicos.					

No	Violación/Vulnerab	Riesgos	Probab	Impact	Políticas y acciones
1	La licencia de Operación de la Red (a partir del Certificado actualizado de Inscripción en el Registro de Redes del MIC).	La licencia de red garantiza un ordenamiento de las redes, no tenerlo puede acarrear la existencia de “redes no autorizadas” y realizar desde ellas a propósitos ilícitos. Puede significar, R1: Accesos no autorizados con pérdida de información.	Baja, el país no lo permite	Alto,	P1: No permitir, Vigilancia y revisión de tráficos o accesos no autorizados en los logs.
2	La existencia del Plan de Seguridad Informática (actualizado) y aprobado por la autoridad facultada.	De no existir en la entidad un PSI o estar desactualizado, la actividad puede: R2: Estar desorganizada, R3: Sin identificarse riesgos, ni tomar medidas preventivas necesarias para evitar pérdida de datos, contaminaciones por virus, etc.	Media	Medio	P2: Revisión periódica del PSI.
3	El nombramiento del Responsable de Seguridad Informática en esta responsabilidad. NOTA: La legislación (127/07) lo define como el especialista encargado de atender la SI, todos somos responsables de cumplir la SI.	De no existir un responsable de Seguridad Informática la actividad puede estar desorganizada y R4: No poder enfrentar adecuadamente los riesgos y las contingencias informáticas.	Media	Alto	P3: Nombrar un al encargado de atender la seguridad Informática.
	La autorización otorgada por el MIC para el Uso y explotación de la Red inalámbrica.	La autorización de empleo de Redes garantiza un uso adecuado del espectro radioeléctrico, es decir R5: No interferir y que no nos interfieran en nuestros servicios, con un mínimo de seguridad.	Media	Alto	P4: Mantener el permiso de red y verificar su operación.

5	El libro de registro, logs, o trazas de los eventos vinculados a la seguridad del último año de operaciones del Sistema	El libro de registro o logs nos permiten identificar comportamientos del servicio de red y conocer las respuestas del sistema ante cualquier incidente. No tenerlo implica que R6: Hacemos una administración ciega de la red, de modo ineficiente e inseguro.	Media	Alta	P5: Establecer un sistema de trazas y logs que guarden los eventos más significativos del SI
6	Existencia de segmentos de red inalámbrica sin la seguridad adecuada.	Esta vulnerabilidad pudiera permitir el R7: Acceso no autorizado para los servicios y contenidos de la red, incluso “hackear” el sistema y sacarlo de servicio.	Alta	Alta	P6: Garantizar niveles adecuados de seguridad en los segmentos inalámbricos.
7	Ubicación del servidor en áreas de acceso colectivo por personal ajeno a esas funciones	Permite el acceso físico y lógico a este posibilitando R8: La ocurrencia de daños físicos (robos, etc.) y R9: Pérdida y/o alteración de datos.	Alta	Alta	P7: Colocar los elementos críticos de la red en locales seguros.
8	Empleo de una laptop personal del director conectada a la red para recibir servicios de correo y navegación	Introducción de malware en la red, puede provocar, R10: Pérdida de información, porque el equipo fuera del dominio no sigue las normas de seguridad.	Alta	Alta	P8: Garantizar que se empleen en la red solo los equipos que están en el dominio.
	El administrador de la red es al mismo tiempo el responsable de la seguridad informática.	Dualidad de responsabilidades que puede permitir al administrador R11: Cometer acciones fraudulentas, como venta de cuentas, acceso remotos, etc.	Alta	Alta	P9: Separar funciones y responsabilida-des
10	Coexistencia en una misma red local de servicios de oficina (navegación y correo, etc.)	R12: Acceso a datos y servicios no permitidos, R13: Congestión de la red, R14: Robo de información, etc.	Alta	Alta	P10: Segmentar la red según las funciones de cada área.

Políticas	**Medidas**

1	El acceso a la red del HMTC se realizará solo por los usuarios registrados desde un segmento seguro y se guardarán las trazas de la actividad. Responsable: Administrador	a	Integrar un mecanismo de trazas de actividad en el segmento de la red segura.
		b	Desarrollar una aplicación para el análisis dinámico de las trazas para alertar en tiempo real acceso no válidos.
2	La sincronización de datos entre los servidores del HTMC y el DATACENTER externo se realizará sobre redes seguras, garantizando la integridad de estos. Responsable: Responsable de seguridad de datos	a	Arrendamiento de un enlace dedicado entre el nodo del HMTC y el data Center solo para esa actividad, implica un alto nivel de seguridad pero estará subutilizado al realizarse la sincronización una vez al día, podría esto extenderse aprovechando esa facilidad.
		b	Creación de una Red Privada Virtual (VPN) sobre Internet entre el nodo y el Data Center. Es una variante que sugiere ser más económica, requiere que los equipos que intervienen en el enlace soporten VPN (Routers, etc), lo que posiblemente implicará su reposición de los actuales.
		c	Implementar IPv6 para elevar la seguridad del enlace.
		d	Solicitar a la autoridad correspondiente la licencia para un servicio de PKI (encriptación de la información) con el enlace actual.
3	Se permitirá la gestión (administración, diagnóstico y reporte) en línea de los equipos médicos del HMTC desde la intranet o internet garantizando solo el acceso del personal autorizado y la integridad de la información médica contenida en ellos. No será posible la reconfiguración de parámetros de operación en modo remoto. Responsable: Técnicos Especializados	a	Crear una red de datos dedicada solo a los equipos médicos y los servicios soportados en ella creando un firewall de seguridad para el intercambio con el resto de la red de modo seguro.
		b	Integrar los mecanismos de acceso a la red de datos, primero en el dominio del HMTC y después en el segmento de red seguro de equipos médicos.
		c	Crear dentro de la subred del área clínica un almacén de datos independiente a los equipos con una copia primaria de estos y que esta sea la que se replique con el server de la DMZ del nodo.

		d	Garantizar con el proveedor/fabricante de los equipos médicos que estos solo puedan configurarse en modo local desde consola, sin configuración remota.

Para mantener y aun mejorar el honor y dignidad de la profesión, y con el objeto de estar a la altura de los altos estándares de conducta ética, en función de la consecución de estos objetivos, y con el ánimo de garantizar el uso apropiado de las mencionadas tecnologías, es que se establece el presente Código de Ética, que será de estricto cumplimiento de todos.

NO.	**CÓDIGO ÉTICA**
1	Aceptar la responsabilidad e la salva y publicación de información.
2	No aplicar tecnologías sin un apropiado conocimiento de la aplicación y desconocimiento de su potencial.
3	Evitar las injurias sobre la reputación de personal con intenciones maliciosas.
4	Las cuentas de los usuarios no deberán utilizarse con fines lucrativos, ilícitos o de índole personal.
5	Los administradores están en la obligación de garantizar la calidad de la información que se genere o reciba en su área de Red.
6	Queda prohibida la distribución de información no acorde con los principios de la Revolución y de información intencionalmente encriptado.
7	Los usuarios y los administradores deben informar de inmediato cualquier violación del presente código a la administración.
8	No se debe realizar ningún tipo de ataque a la seguridad informática de sistemas locales o remotos, así como el envío o reenvío de mensajes masivos con información intrascendente.
9	Observar una conducta personal que le haga acreedor del respeto de sus conciudadanos.
10	No alterar, manipular o falsear datos o informaciones a las que haya tenido acceso.
11	Contribuir con la sociedad y con el bienestar de la humanidad.
12	Respetar la privacidad ajena.
13	Conocer y respetar la existencia de leyes para el trabajo profesional.
15	El acceso a los recursos de computación y las comunicaciones solo cuando han sido autorizados.