	HOSPITAL UNIVERSITARIO DEL VALLE "EVARISTO GARCIA" E.S.E	**CÓDIGO:**	MOP-GDI-SIS-002
		VERSIÓN:	001
	PLAN ESTRATÉGICO DE TECNOLOGIAS DE LA IN	**FECHA DE EMISIÓN:**	2019-05-22

1. OBJETIVO

El objetivo del Plan Estratégico de las Tecnologías de la Información y Las Comunicaciones – PETI del Hospital Universitario del Valle “Evaristo García” E.S.E., es orientar la toma de decisiones y proveer los lineamientos en cuanto a gestión de TICS en la organización, garantizando siempre la integridad, seguridad y accesibilidad de la información para generar valor en los procesos beneficiando siempre al usuario de servicios en la institución.

2. NORMATIVIDAD

Ley 1266 de 2008: Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1437 de 2011: Por la cual se expide el código de procedimiento administrativo y de lo contencioso administrativo.

Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.

Ley 1753 de 09 de junio de 2015: Por la cual se expide el Plan Nacional de Desarrollo, 2014-2018. “Todos por un nuevo país”.

Decreto 3816 de 2003: "Por el cual se crea la Comisión Intersectorial de Políticas y de Gestión de la Información para la Administración Pública".

Decreto 235 de 2010: Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones.

Decreto 019 de 2012: Por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.

Decreto 1080 de 2015: Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Decreto 1078 de 2015: "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

Decreto 415 de 2016: "Por el cual se adiciona el Decreto Único reglamentario del sector de la Función Pública, Decreto 1083 de 2015, en lo relacionado con la definición de lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones".

Decreto 2094 de 2016: Por el cual se modifica la estructura del Departamento Administrativo para la Prosperidad Social.

Decreto 1499 de 2017: Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Documento CONPES No. 3854 de 2016: Política Nacional de Seguridad Digital.

Acuerdo 003 de 2015 del AGN: “Por el cual se establecen los lineamientos generales para las

entidades del Estado en cuanto a la gestión de documentos electrónicos generados como resultado del uso de medios electrónicos de conformidad con lo establecido en el capítulo IV de la Ley 1437 de 2011, se reglamenta el artículo 21 de la Ley 594 de 2000 y el capítulo IV del Decreto 2609 de 2012.

3. DEFINICIONES

Activo de información: Cualquier componente (Humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios del hospital y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: Es un documento en los que los funcionarios del HUV o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad de la información: Proceso sistemático de identificación de fuentes, estimación de impactos, probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: Es el procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Centros de cableado: Son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: Es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: Es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad.

Confidencialidad: Es la garantía de que la información no está disponible o divulgada a personas, entidades o procesos no autorizados.

Control: Es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye politícas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: Es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación y su uso no autorizado.

Derechos de Autor: Es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: Es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: Dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Hardware: Refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.

Incidente de Seguridad: Es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, la consecuencia, el número de veces ocurrido o el origen (interno o externo).

Informática: La informática es una ciencia que estudia métodos, procesos, técnicas, con el fin de

almacenar, procesar y transmitir información y datos en formato digital.

Integridad: Es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: Es una lista ordenada y documentada de los activos de información pertenecientes al hospital.

Licencia de software: Es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: Es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros, CDs, DVDs y unidades de almacenamiento USB.

Perfiles de usuario: Son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: Es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: Es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: Son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior del HUV.

Registros de Auditoría o Log: Son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos del hospital. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: Es la persona o grupo de personas, designadas por los altos mandos, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

PSGI: Políticas de Seguridad de Gestión de la Información.

Sistema de información: Es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por el HUV o de origen externo ya sea adquirido por la entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental: Son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Software: Equipamiento lógico o soporte lógico de un sistema informático, que comprende el conjunto de los componentes lógicos necesarios que hacen posible la realización de tareas específicas.

Software malicioso: Es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Tecnología: Es el conjunto de conocimientos técnicos, ordenados científicamente, que permiten diseñar y crear bienes y servicios que facilitan la adaptación al medio ambiente y satisfacer tanto las necesidades esenciales como los deseos de la humanidad.

Terceros: Todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que

provean servicios o productos a la entidad.

Vulnerabilidades: Son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por el hospital (amenazas), las cuales se constituyen en fuentes de riesgo.

4. RESPONSABILIDAD

Persona o equipo responsable de la implementacion del manual

5. CONTENIDO

RUPTURAS ESTRATÉGICAS

Las Rupturas estratégicas identificadas que permitirán la transformación de la gestión de TI en la institución son:

- La gestión de TI requiere una gerencia integral que dé resultados. Contar con una oficina de TI, que haga parte del comité directivo, que gerencia las actividades, los recursos y que se enfoque hacia un servicio de la mejor calidad posible, para los clientes internos y externos.
- Existe la necesidad de integrar las acciones, los presupuestos y los proyectos para generar economías de escala, crecimiento ordenado y especialización.
- Aumento en la capacidad de análisis de información. Impulsar el desarrollo de las capacidades analíticas en cuanto a: herramientas, personal, resultados y publicación.
- Contar con el liderazgo al interior de la entidad para la gestión de sistemas de información.
- Se requiere un líder que entienda el sector, con habilidades multidisciplinarias; con pensamiento sistémico y sistemático; facilitador y potenciador de la eficiencia en los procesos y de la transparencia en la gestión; practicidad / Orientación a resultados; con experiencia en cargos de liderazgo y conocimiento del sector privado y público.
- Necesidad de definir estándares de integración e interoperabilidad.
- Integración entre las fuentes de datos y las herramientas de consolidación.
- Miradas holísticas.
- Silos de información
- Fortalecer el equipo humano y desarrollar sus capacidades de Uso y Apropiación de TIC.
- Aumentar la cantidad y las competencias tanto de personal de planta y de contratistas. Integrando a los proveedores en la generación de valor.
- Desarrollar una cultura digital al interior de la entidad.
- Realizar una comunicación interna intensa y creativa sobre la adopción de TIC en la gestión.
- Adelantar una estrategia de Uso y Apropiación sectorial hacia la comunidad

ANÁLISIS DE LA SITUACIÓN ACTUAL

Estrategia TI

El Hospital Universitario del Valle “Evaristo García” E.S.E., es una Empresa Social del Estado de carácter departamental, con patrimonio propio, autonomía administrativa y presupuestal. Tiene un área construida de aproximadamente 52.000 metros cuadrados, presta los servicios de: urgencias, hospitalización adultos y pediátricos, unidades de cuidados intensivos adultos, recién nacidos, medicina física y rehabilitación, laboratorios, imagenología, banco de sangre, endoscopia, oncología pediátrica y adulta, quimioterapia, radioterapia, salas de cirugía, consulta externa especializada, atención a la madre gestante, al recién nacido, entre otros servicios como ortogeriatría, mama canguro, lactancia materna segura, amigos de la mujer y la infancia (IAMI), atención integral al paciente quemado. Orienta su portafolio de servicios a la comunidad del Valle del Cauca y el suroccidente colombiano; es una institución que ha luchado por modernizar sus instalaciones y su tecnología, atiende una gran población subsidiada y población vulnerable sin capacidad de pago, su compromiso con la comunidad es la oportunidad, la eficacia y en general con la calidad de la atención.

Como entidad formadora el HUV desarrolla un programa competitivo de corte educativo que permite atender las demandas sociales de perfeccionamiento profesional, técnico, operativo y especializado, partiendo de la imagen corporativa del Hospital y la integración de tecnología, infraestructura y talento humano. Procesos dinámicos que permiten generar conocimientos, perfeccionar habilidades y vislumbrar actitudes de corte humanista, absolutamente indispensables para proyectarse a una sociedad ávida de ayuda y de orientación. Actualmente el Hospital cuenta con veintitrés (23) Convenios institucionales de

prácticas de aprendizaje con Universidades y Escuelas, mediante el diseño y cumplimiento a corto, mediano y largo plazo, de planes orientados a intervenir las necesidades educativas del Hospital. Principalmente desarrolla convenios nacionales con la Universidad del Valle, Universidad Santiago de Cali, Pontificia Universidad Javeriana, Universidad San Buenaventura, Universidad Católica de Manizales entre otras importantes instituciones de educación superior. Así mismo, es centro de prácticas de escuelas de enfermería entre ellas Comfenalco, Intenalco, Fátima, FUNAP, Humanizar, edén, Sena entre otras.

Ofrece además la posibilidad de adelantar por contactos nacionales e internacionales para generar conocimientos en el intercambio de profesionales de la salud en la modalidad de pasantías en Urgencias-Unidad de Trauma, Unidades de Terapia Intensiva, Ginecoobstetricia, Pediatría - Sirena, Medicina Interna, Neurocirugía, Ortopedia, Sala de Operaciones, Quirúrgicas -Quemados y Epidemiología Hospitalaria. Se ofrecen programas de educación no formal para profesionales en las diferentes especialidades, profesiones y técnicos: Diplomados, Congresos, Simposios, Curso –Taller, Diplomado en urgencias para Auxiliares, Diplomado en Urgencias para Médicos y otros. El Hospital cuenta con un Sistema Políticas de Gestión de seguridad de la Información PSGI conformada por:

- Política de Seguridad en la red
- Política de Seguridad de del Centro de Cableado y Datos
- Política de Seguridad de Equipos
- Política de establecimiento, uso y protección de claves de acceso
- Política de Seguridad del Personal
- Política de Gestión de activos de la Información
- Política de manejo de la Información.
- Política de control de Acceso.
- Política de Acceso Remoto.
- Política de encriptación y Criptografía.
- Política de seguridad física y medio ambiente
- Política de Seguridad Operativa
- Política de seguridad en las comunicaciones
- Política de Desarrollo Sistemas de información
- Política de Seguridad con terceros
- Política de Gestión de Riesgos
- Política de Control de Backup
- Política de Planes de Contingencia

El Hospital Universitario del Valle “Evaristo García” E.S.E. a través del Sistema de políticas de seguridad de la información establece medidas y patrones de administración y organización tanto de las Tecnologías de Información y Comunicación TIC´S como toda la Seguridad física de la Información.

Uso y Apropiación de la Tecnología

Para lograr un adecuado uso y apropiación de la tecnología, actualmente el HUV, realiza programas de inducción, capacitación y reinducción de los sistemas de información y herramientas tecnológicas al personal nuevo y antiguo; de igual forma se cuenta con una red local, la cual sirve como herramienta indispensable, para que cada uno de los usuarios puedan tener acceso a información que tiene expuestos diversos temas sobre los servicios TI ofrecidos, como lo son políticas de seguridad de la información, uso de sistemas de información, entre muchos otros documentos con contenido relevante para la institución.

Sistemas de Información

LOCALIZACION: Centro de datos único situado en el edificio del Hospital Universitario del Valle “Evaristo García” E.S.E

- El espacio físico
- Las adecuaciones básicas
- La seguridad

EQUIPAMIENTO: Elementos de infraestructura de tipo Hardware como son servidores y sistemas de almacenamiento.

COMPUTO:

- Servidores tipo Blade
- Chasis HPE Blade Server c3000
- 7 Servidores basados en Intel x86
- 3 con capa de virtualización KVM
- 4 físicos
- Chasis HPE BLAde Server C7000

- 7 servidores basados en Intel x86
- 6 servidores con capa de virtualización VMWAre
- 2 Clusters VMWARE con 3 servidores cada uno
- 1 Servidor físico
- Servidores tipo Rack
- Ambiente heterogéneo con hardware de servidores marca HPE y Dell
- Servidor HPE DL180
- Servidor HPE DL320
- Servidor HPE DL120
- Servidor Dell 610
- Servidor Dell 710
- Servidor Dell 520
- Servidores tipo Torre
- Ambiente heterogéneo con hardware de servidores marca HPE y Dell. Además de los fabricantes predominantes, se encuentra un servidor con marca indeterminada
- Servidor Dell 2900
- Servidor Dell 2900
- Servidor Caja Blanca
- Servidores tipo Desktop
- Se utiliza hardware de equipos de escritorio, no fabricados con roles de servidor Desktop HP – Intranet
- Desktop HP – Servidor de archivos
- Desktop HP

ALMACENAMIENTO:

- Sistema de discos tipo SAN (presenta bloques mediante FC)
- HPE 3PAR
- Espacio total aproximado 9,6TB
- Espacio asignado 9,3TB
- Espacio disponible 2,7%
- HPE EVA 4400
- Espacio total aproximado 5,7TB
- Espacio asignado 4,5TB
- Espacio disponible 26,7%
- Sistema de discos tipo NAS (presenta sistema de archivos mediante red LAN)
- Lenovo 4610 – Imágenes
- Gestionado por terceros
- Sistema de almacenamiento en cintas magnéticas
- Dell TL2000 – Backup
- RED
- Conmutadores de red (núcleo)
- 2 Cisco Catalyst 3750 - Apilable

VIRTUALIZACION:

- Software para optimización y consolidación de servidores VMWare y KVM Ambiente KVM sobre 3 servidores Blade HPE en el C3000, que contiene máquinas virtuales.
- Ambiente VMWAre sobre 6 servidores Blade HPE en el C7000 distribuidos en 2 clusters, uno para aplicaciones de Servinte anterior al productivo y el otro donde corre capas diferentes a base de datos del Servinte productivo.

SOFTWARE OPERACIONAL: Sobre servidores físicos y virtuales

- Linux Server con predominio de Suse u otras distribuciones libres Ninguno con suscripción vigente
- Microsoft Windows Server de diferentes versiones y ediciones Ninguno con seguro de software

SOFTWARE APLICATIVO:

- Sistema de núcleo de negocio Servinte
- Ambiente productivo
- Ambiente de pruebas
- Histórico
- Base de datos Informix
- Datos de pruebas y producción sobre el sistema de discos 3PAR
- Datos históricos sobre el sistema de discos EVA4400
- Sistema de gestión documental DOCUNET: Base de datos Oracle, Datos sobre el sistema de discos

EVA4400
- Sistema de gestión de calidad DARUMA: Base de datos Oracle, Datos sobre el sistema de discos EVA4400
- Sistema de gestión de PQRS Cross: Base de datos Postgre SQ, Datos sobre el sistema de discos EVA4400
- Sistema de PACS (Picture Archiving and Comunications System Sistema de archivos, Datos sobre el sistema de almacenamiento compartido Lenovo NAS 4610
- Sistema de correo electrónico Horde, Base de datos de correos, Datos sobre el sistema discos EVA4400, Datos sobre el sistema de discos 3PAR

CAPA DE DATOS: Donde se conservan los datos productivos relacionados con las aplicaciones más importantes

- DARUMA base de datos Oracle
- DOCUNET base de datos Oracle
- SERVINTE base de datos Informix
- CROSS base de datos PostgreSQL

HERRAMIENTAS DE GESTION: Se cuenta con herramientas básicas de gestión en cada una de las capas

1. El cómputo se gestiona mediante el firmware de cada servidor o en el caso de los Blades en sus módulos de administración
2. Los sistemas de almacenamiento tipo SAN/NAS se administran mediante sus sistemas operacionales directamente
3. El sistema de cintas magnéticas se administra a través de su firmware y en los sistemas operacionales mediante los controladores de cada uno
4. Los conmutadores de red mediante su sistema operacional propietario
5. Las herramientas de virtualización cuentan con sus consolas de gestión cada una
6. Los sistemas operacionales mediante sus propias herramientas administrativas

- No se cuenta con una herramienta de monitorización
- No se cuenta con elementos de telemetría ni comportamiento
- No se cuenta con herramientas que apoyen la gestión de la capacidad

SEGURIDAD: Seguridad de red para prevenir ataques informáticos de diferentes índoles y seguridad de los datos para garantizar su disponibilidad e integridad.

Directorio Activo: Se implementó un esquema de directorio activo de Microsoft

1. Sistema operacional Windows Server 2008R2
2. Corre sobre uno de los servidores DL460 del sistema blade C7000
3. Los datos se encuentran alojados sobre el sistema de discos 3PAR

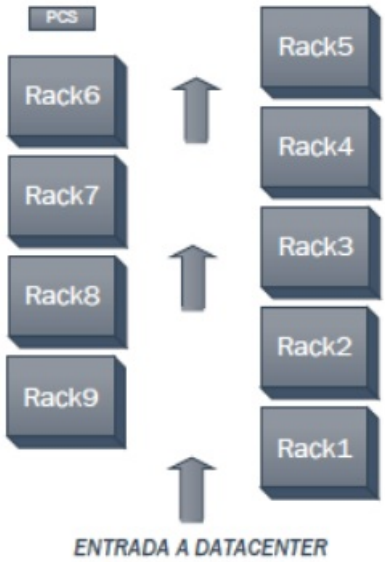
Seguridad de red: Se dispone de un equipo tipo UTM marca Sonicwall de rango medio

1. Está en ambiente de alta disponibilidad
2. Es de capa 7 con integración con sistemas de identificación como LDAP o Microsoft DA
3. Se le destina además roles de enrutamiento entre las diferentes redes virtuales

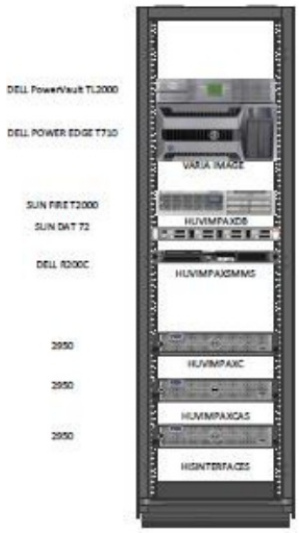
Seguridad de los datos: Se carece de herramienta de automatización de copias de respaldo

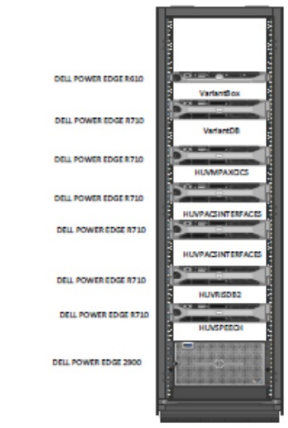
1. Se hacen copas de respaldo con herramientas nativas de los sistemas operacionales, los manejadores de bases de datos y aplicaciones
2. Se carece de un plan de recuperación ante desastres
3. Se cuenta con replicaciones entre bases de datos con herramientas nativas

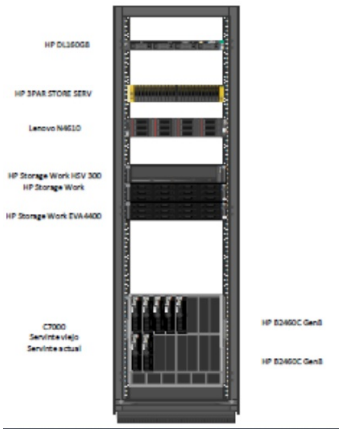
Para los sistemas que gestionan terceros como PACS, RIS y Radioterapia, se entrega la responsabilidad de efectuar las copias de respaldo.

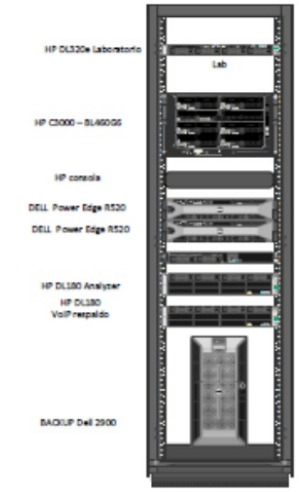


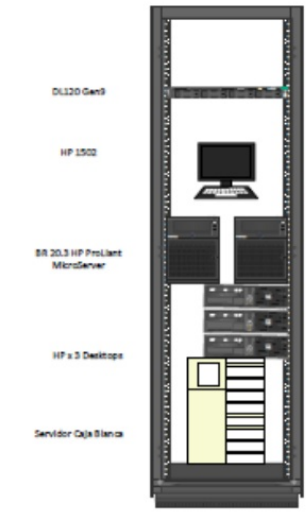
Estos sistemas se encuentran inactivos en su mayoría por problemas contractuales entre el proveedor y el HUV.

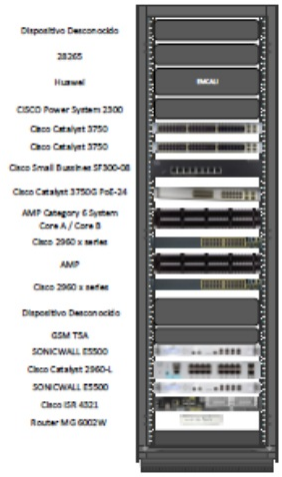


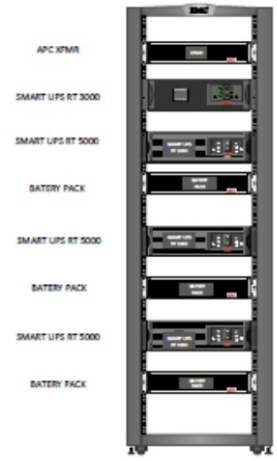

DELL POWER EDGE R610
DELL POWER EDGE R710
DELL POWER EDGE R710
DELL POWER EDGE R710
DELL POWER EDGE R710
DELL POWER EDGE R710
DELL POWER EDGE R710
DELL POWER EDGE 2900
VariantBox
VariantDB
HUMMPAXOCS
HUVPACSINTERFACES
HUVPACSINTERFACES
HUVRISDB2
HUMSPEECH

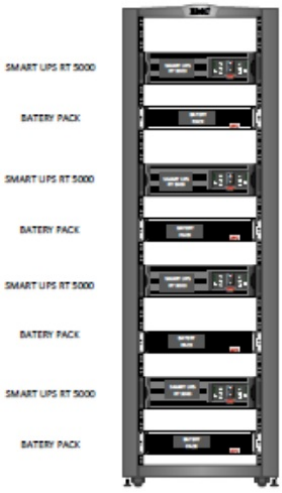

HP DL160G8
HP 3PAR STORE SERV
Lenovo N4610
HP Storage Work HSV 300
HP Storage Work
HP Storage Work EVA4400
C7000
Servinte viejo
Servinte actual
HP B2460C Gen8
HP B2460C Gen8

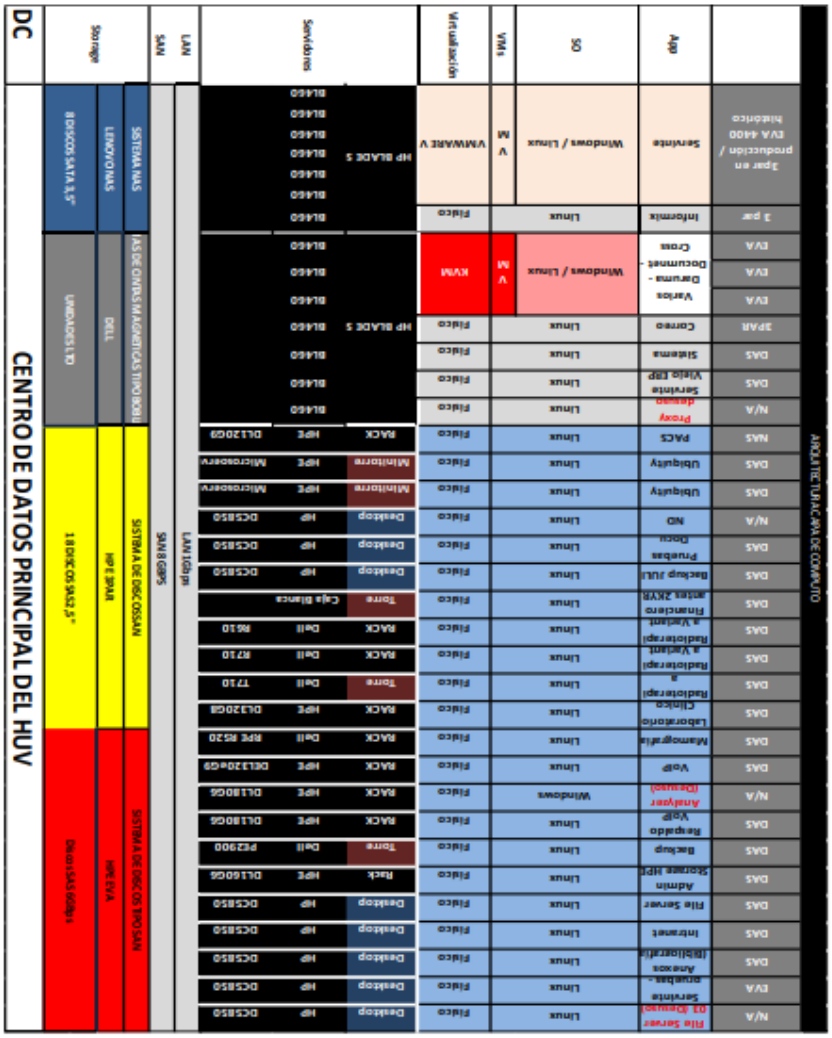

HP DL320e Laboratorio
Lab
HP C3000 – BL460G6
HP consola
DELL Power Edge R520
DELL Power Edge R520
HP DL180 Analyzer
HP DL180
VoIP respaldo
BACKUP Dell 2900


DL120 Gen9
HP 1502
BB 20.3 HP ProLiant
MicroServer
HP x 3 Desktops
Servidor Caja Blanca


Dispositivo Desconocido
28265
Huawei
EMCAU
CISCO Power System 2300
Cisco Catalyst 3750
Cisco Catalyst 3750
Cisco Small Bussines SF300-08
Cisco Catalyst 3750G PoE-24
AMP Category 6 System Core A / Core B
Cisco 2960 x series
AMP
Cisco 2960 x series
Dispositivo Desconocido
GSM TSA
SONICWALL E5500
Cisco Catalyst 2960-L
SONICWALL E5500
Cisco ISR 4321
Router MG 6002W


APC XRMR
SMART UPS RT 3000
SMART UPS RT 5000
BATERY PACK
SMART UPS RT 5000
BATERY PACK
SMART UPS RT 5000
BATERY PACK


SMART UPS RT 5000
BATERY PACK
SMART UPS RT 5000
BATERY PACK
SMART UPS RT 5000
BATERY PACK
SMART UPS RT 5000
BATERY PACK



Centro de datos:

- Los sistemas de adecuación del centro de datos como las unidades de ininterrupción de potencia (UPS) y refrigeración no están cubiertos por garantía, no se hizo extensión de la misma y no se tiene un contrato de asistencia técnica que garantice una oportuna reacción ante un imprevisto.
- El sistema de apagado de incendios no tiene un mantenimiento adecuado por lo que no se garantiza su funcionamiento en caso de necesitarse.
- Este sistema funciona por sustracción de oxígeno, por lo que mantenerlo es indispensable, además se debe garantizar pleno vacío en el centro de datos para su operación, lo que no veo posible.

Equipamiento:

Computo:

- Por la edad dentro del ciclo de vida productivo de la gran mayoría de los elementos de infraestructura se pueden presentar problemas atribuibles al hardware, sobre todo en aquellos que tienen partes electromecánicas.
- Blade Servers – Los sistemas C3000 y C7000 no cuentan con garantía vigente y no hicieron extensión de la misma, el fabricante ya no permite suscribir garantía de estos sistemas y sus componentes (chasis, administración, computo, entrada y salida, y almacenamiento).
- Los equipos de gabinete o rack, con excepción de un HPE DL320G9, que es administrado por terceros, en su totalidad excedieron los tres años de funcionamiento, no se les extendió el periodo de garantía con cada uno de los fabricantes y por la edad de sus componentes, ya deben sufrir deterioro por desgaste de materiales.
- Los equipos de torre, aunque en mucha menor cantidad, presentan la misma situación que los de rack.
- Los equipos Desktop (escritorio) también superar la expectativa de ciclo de vida, con el agravante de que sus componentes no fueron hechos para asumir roles de servidores.

Almacenamiento:

- El HPE 3Par que contiene gran parte de la información sensible excedió en periodo de garantía, no se renovó con el fabricante, tiene en más del 80% de sus elementos piezas móviles (mecánicas) por lo

que el deterioro es mayor Su capacidad está casi siempre por encima del 95%, esto hace que funcione con mayor lentitud y pudiese colapsar.
- EL HPE EVA4400 está retirado del mercado, está fuera de su cobertura de garantía, su tiempo de utilización es mayor que el 3Par, por lo que se puede suponer con gran certeza que existe un gran desgaste de sus componentes electro-mecánicos Su capacidad está sobre el 74% de consumo.
- El Lenovo NAS 4610 está dentro de su ciclo de vida útil, adicionalmente es gestionado por terceros, y todavía cuenta con capacidad de crecimiento importante.
- La biblioteca de cintas Dell está fuera de cobertura de garantía, las cabezas de lecto/escritura tienen un ciclo de vida definido por uso y no tiempo, por lo anterior podemos anticipar se encuentra fuera de su tiempo estimado de utilización.

Riesgos:

Equipamiento

Computo:

- Equipos Blade Server C7000 y C3000 – En este tipo de arquitecturas, los riesgos pueden ser mayores ya que tiene elementos comunes como módulos de administración, redes LAN y SAN, fuentes de poder y ventilación. Aunque tienen elementos redundantes.
- Equipos tipo Rack: Con excepción de un servidor HPE de última generación y el sistema NAS 4610, todos los servidores están fuera de los términos de garantía, tampoco se les contrató extenderla, no cuentan con un plan de mantenimiento y no disponen de un plan de asistencia. Muchos de estos equipos, por su prolongado tiempo de utilización, podrían tener mucho desgaste en sus materiales, además de la gran dificultad de localizar repuestos en caso de requerirse
- Equipos tipo Torre: Hay pocas unidades, todos en situación parecida a la de los servidores de Rack, uno bastante crítico, es un servidor que corre un aplicativo financiero histórico (no en producción) al que llamaremos “caja blanca” ya que no es determinante su marca y modelo, es evidente el deterioro y la caducidad de su tecnología
- Equipos tipo Desktop: Se ha destinado roles de servidor a varios equipos de escritorio, es importante recalcar que su arquitectura y componentes no corresponden a la función que se les asignó. Sus materiales y su arquitectura no están hechos para soportar estas cargas de trabajo y menos para correr en jornadas 7x24

Almacenamiento:

Sistema de disco HPE 3PAR

- Se encuentra con cerca del 97% de su capacidad agotada. Está en la fase productiva con más de 2/3 de su ciclo consumido, esto quiere decir que está llegando al final de su ciclo de vida
- Por su naturaleza y el tipo de elementos que lo conforman, donde predominan discos mecánicos, se puede pronosticar una alta probabilidad de falla
- Como es un elemento común para aplicaciones de misión crítica y de uso colectivo se considera de alto impacto
- El nivel de riesgo es alto

Sistema de discos HPE EVA4400

- Tiene consumido el 74% de su capacidad de almacenamiento
- Cuenta con su ciclo de vida ya cumplido (más del 100%)
- Muchos de sus discos, todos mecánicos, ya están cercanos o superaron la expectativa de uso del fabricante, por lo que el pronóstico de fallas es inminente
- En caso de que ocurran desperfectos la consecución de repuestos es difícil, bastante costosa en caso de acudir al fabricante o muy riesgosa en caso de mercado de re-manufacturados
- Aun soporta aplicaciones en etapa productiva
- Dado a que su utilización es colectiva, el nivel de impacto de un fallo es alto
- El nivel de riesgo en muy alto.

Sistema de discos tipo NAS Lenovo

- Se encuentra dentro de su ciclo de vida productivo en tiempo menos a la 1/3 parte
- Dispone de garantía por parte del fabricante
- Está delegado en terceros por lo que el HUV no asume el ciclo de vida

Sistema de almacenamiento en cintas magnéticas Dell

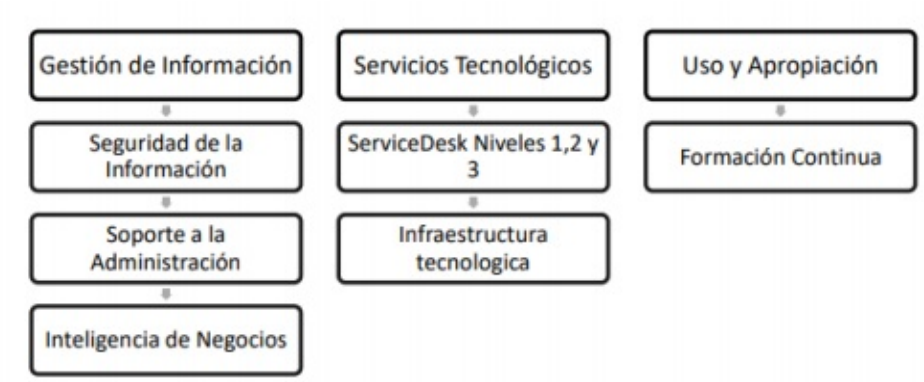
- No cuenta con cobertura de garantía vigente por el fabricante
- Las cabezas de lecto/escrituras tienen una expectativa cerrada de grabaciones:
- No se cuenta con esta información

- Podría haber superado su umbral
- El nivel de impacto es medio
- Se considera un elemento de riesgo medio

Red

- Equipos cisco Catalyst 3750
- Sin cobertura de garantía por parte del fabricante
- Sin posibilidades de actualización a ultimo nivel de tecnología disponible
- En esquema de apilamiento que mitiga riesgos
- Muy críticos para la operación
- El nivel de riesgo se considera alto

MODELO DE GESTION DE TI



Linea de Servicio	Descripción	Actividades Realizadas
Seguridad de la Información	Línea de servicio especializado en ISO 27001 encaminado a la gestión del Sistema de Gestión de Seguridad de la Información, con el objetivo de proponer y gestionar un conjunto de controles lógicos, físicos y administrativos.	• Controles de Seguridad de la Información. • Analisis y reporte de Incidentes relacionados con la Seguridad de la Información. • Generar matriz de riesgos de la seguridad de la información. • Planes enfocado al mejoramiento de la seguridad e integridad de la información. • Plan de Capacitaciones. • Indicadores
Soporte a la Administración	Línea de servicio encargado de asesorar, evaluar, y emitir conceptos relacionados con el uso de las diferentes herramientas informáticas.	• Acompañamiento en diferentes proyectos de mejoramiento y toma de decisiones en la gestión de la Información. • Estrategia de adopción e implmentación de la Estrategia de Gobierno Digital. • Actualización de procedimientos TIC (Manual de Procedimientos). • Implementación de la plataforma E-Learning.
Inteligencia de Negocios	Línea de servicio encargado del mantenimiento de la plataforma de inteligencia de negocios del hospital, ajusta o crea nuevos indicadores y colabora de forma efectiva con las otras áreas en la generación de informes que permitan mejorar la productividad de los equipos.	• Identificación de requerimientos. • Identificar Origen del dato. • Definir esquema logico. • Diseño y creación de la solución. • Despliegue de paquetes de extracción de pruebas. • Pruebas al Modelo.

Fuente. Líneas de Servicio Service Desk

Gestión de Información

Se cuenta con una infraestructura heterogénea y bastante fragmentada y con un alto nivel de complejidad, producto aparentemente de poca planeación que desembocan en grandes dificultades para gestionarla.

En términos generales se puede concluir que el HUV corre riesgos inminentes en el desarrollo de su negocio atribuible al estado actual de su infraestructura de tecnología informática y comunicaciones.

Dispone de activos que ya acusan niveles altos de obsolescencia, es generalizada la falta de cobertura de garantía y el desgaste es bastante evidente, las capacidades ya las desbordaron teniendo que poner en funcionamiento equipos no adecuados para los roles que se les asignan, además ya las aplicaciones acusan un rendimiento insuficiente para satisfacer las expectativas de los usuarios.

No se ha diseñado, o por lo menos no se implementó una estrategia apoyada en mejores prácticas para la gestión de tecnología, se hace muy confusa y compleja la operación, además de bastante vulnerable ante errores.
A pesar de los altos niveles de riesgo que se corre, no hay un plan claro de mitigación de los mismos. El HUV no está preparado para un incidente catastrófico que afecte su infraestructura de TIC, sin importar si es de orden menor o mayor.
La seguridad de la red es aceptable, se dispone de elementos con suficiente alcance para su salvaguarda, su usabilidad podría ser mejor, aunque se presenta la misma situación que en los otros activos de TIC, ya los modelos están descontinuados en el mercado y se pronostica la falta de soporte por parte del fabricante.
No se tiene tampoco una estrategia clara de respaldo y recuperación de la información, las actividades que se desarrollan cotidianamente están bastante lejanas de las que requiere la organización, el objetivo de pérdida de información no está determinado y la práctica actual no es garantía de tranquilidad, los objetivos de tiempo de recuperación de los servicios informáticos dejan ver una brecha entre lo empírico y lo requerido.
Ningún sistema operacional o el software de virtualización cuenta con suscripciones de software vigente, esto hace que no se pueda mantener los niveles de tecnología adecuados, lo que genera grandes vectores de riesgo, además de no poder contar con soporte en ningún nivel de parte de cada uno de los fabricantes, haciendo inoportuna una intervención en momentos de crisis.
Uno de los peores escenarios es en las capas medias y bases de datos, ningunos de los productos cuenta con mantenimiento activo, lo que concuerda con sus aplicaciones, donde la situación es la misma, en algunos productos ya se puede decir que se perdió el licenciamiento por los altos costos de restablecimiento, lo más inquietante es que no se cuenta con ningún nivel de escalamiento en caso de requerirlo.

Gobierno de TI

La persona responsable por parte del HUV, es el Jefe de la Oficina de gestión de la información, quien aprueba y autoriza las decisiones en cuanto al área se refiere. Es también el representante de la alta dirección y el interlocutor entre TIC y la gerencia.
Existen en la actualidad un esquema de Service Desk que presta los servicios de soporte técnico y mantenimiento de la infraestructura tecnológica física y lógica bajo el modelo de Gestión ITIL.

Planeación Estratégica de TIC

Se determina el problema principal la falta de planeación de tecnología, lo que conlleva a problemas asociados como son una gestión inadecuada que se aleja de las mejores prácticas, costos descontrolados, altos riesgos de interrupción de los servicios y pérdida de información relevante y la imposibilidad de garantizarle los niveles de servicio a los usuarios directos e indirectos.
La carencia de un plan implica que todo se puede ir volviendo caótico, no hay maneras de alinearse con el direccionamiento de la organización, impidiendo el gobierno de TI, aunque la selección de las aplicaciones misionales o no, apoyen procesos, no se logra una armónica correlación entre estos.
La óptica de la brecha entre el desarrollo del negocio y la tecnología que no solamente lo soporta, sino que debería ser, en su mejor expresión, un elemento promotor de innovación y generador de ingresos, no es clara.

MODELO DE GESTIÓN DE TIC

No se cuenta con un método implementado que garantice la operación en aspectos relevantes como disponibilidad, salubridad, capacidad, cambio, servicios y la seguridad como mínimo, aunque se desarrollen algunas actividades básicas planeadas, el resto se le deja al azar. No se evidencia implementación ni por empoderamiento, ni por documentación.
Lo anterior nos implica cargas de trabajo desbalanceadas, sensación de exceso, pero con resultados precarios, todos los elementos de infraestructura se gestionan por separado, haciendo difícil la determinación precisa de los roles y por ende de los niveles de impacto para la organización.
No se dispone de elementos de tecnología que faciliten la operación, so se hace monitorización ni siquiera a nivel de silos o de capas completas, mucho menos a nivel integral, lo que desemboca en un servicio correctivo o de reacción que repara pero que, al hacerlo, causa deterioros en su prestación.
Con una gestión inadecuada siempre va a haber sensación de caos y de insuficiencia de recursos importantes como es, por ejemplo, personal y entrenamiento.

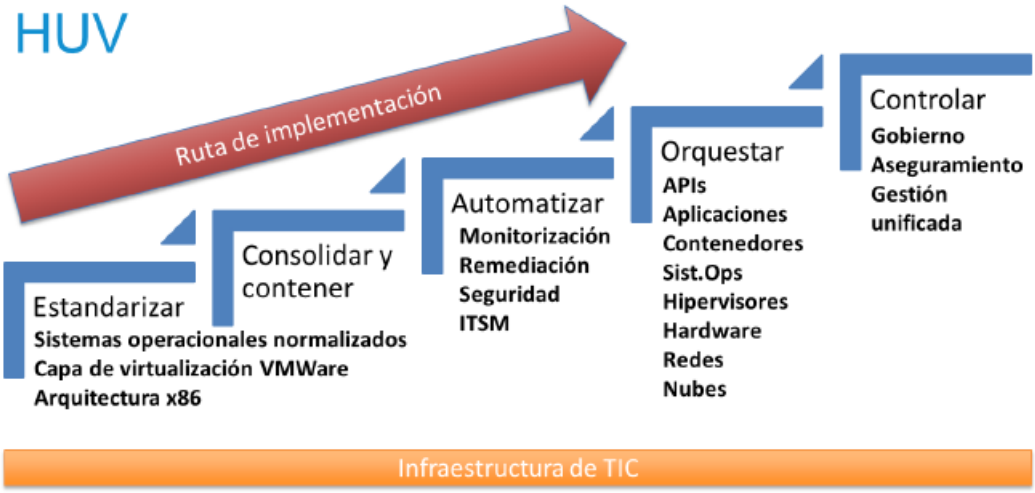
Costos no Controlados

La carencia de una planeación trae como consecuencia la falta de presupuesto o el cálculo no preciso de este, esto hace que el aprovisionamiento de tecnología se haga como un accidente, y no completando un proceso sano, sin análisis de requisitos de nuestro cliente interno, tampoco mediante un estudio adecuando e integral del mercado y lo más grave aún, con un requerimiento formal de oferta a los proveedores inexacto, lo que deja un gran campo de incertidumbre para el resultado final.
Se debe tener presente y claro que unos son los costos de adquisición y capital, y otros los de pertenecía asociados al asumir la gestión del ciclo de vida de los elementos de infraestructura, siempre hay una gran relación entre unos y otros.
Los costos finalmente deben estar orientados a unidades de negocio o centros de utilidad, deben apoyar como mínimo el desarrollo eficiente y efectivo de los procesos del negocio.

Otra problemática que se desprende es la de costos inesperados y escondido atribuibles a la indisponibilidad de algunos de los servicios que apoya la misión de la organización, estos pueden ser de cuantía importante y de alto impacto, llegando inclusive a poner en riesgo la viabilidad del negocio, ya que provienen de sanciones por incumplimiento de regulaciones y/o leyes, o inclusive por demandas propias de la naturaleza del negocio.
Riesgos:
Los riesgos directamente relacionados con la infraestructura de TIC son los de la no disponibilidad de los servicios informáticos y de los datos, como también los de la pérdida, la fuga, calidad o no integralidad de la información.
Debido al rol de la infraestructura, que fundamentalmente es el de soportar las aplicaciones que apoyan el desarrollo de cada uno de los procesos de la organización, sin importar si son de la cadena de valor o direccionales o de apoyo, su correcta y permanente operación, impacta de manera muy importante el trascender la operación del negocio.
Luego podemos determinar que los riesgos son de muy alto impacto para la organización y sin importar cuál es el origen de su causa, el efecto compromete su viabilidad.
Niveles de servicio:
Se debe garantizar el cumplimiento de los acuerdos operacionales entre los diferentes actores o recursos de los procesos, estos deben ser claramente definidos y de fácil medición, además debe haber elementos para su análisis, desafortunadamente no se evidenció documentación al respecto, ni tampoco de manera empírica, más allá, de la consciencia que tienen los funcionarios del área sobre disponibilidad, desempeño y tiempos de respuesta cuando se presentan incidentes o se debe hacer manejo de crisis.
Al no haber indicadores, no hay medición y por ende objetivo, luego no puede haber criterios para determinar los acuerdos de nivel de servicio, todo se resume a la experiencia del usuario, que además se manifiesta de manera caótica como consecuencia del desgaste en el desarrollo de sus actividades, y se le da un tratamiento reactivo básicamente.

Estrategia de TI

Disponer de una infraestructura de tecnología informática que, por sus características, permita una estrategia de Gobernanza, brindando posibilidades al personal del área de enfocarse en el negocio, asumiendo el rol de impulsadores de innovación que permita la diferenciación y así ofrezca ventaja competitiva mejorando su posición en el mercado y como consecuencia obteniendo mejores ingresos, garantizando más allá de la viabilidad del Hospital, su sano crecimiento.



La infraestructura de TIC debe construirse sobre los siguientes tres pilares fundamentales:

- Mitigación de riesgos
- Eficiencia en costos
- Mejoramiento de los Niveles de Servicio

Objetivos Estratégicos de TI

Consolidación y aseguramiento de la infraestructura de TIC: Implementar una infraestructura de TIC que cumpla con los pilares fundamentales de arquitectura mencionados en el punto anterior, de tal manera que se pueda adquirir con costos eficientes, reduciendo en lo posible las brechas de inseguridad e incrementando los niveles de servicio ofreciendo una gran experiencia de usuario.
El objetivo se puede lograr desarrollando una estrategia de Normalización, Consolidación y Aseguramiento, que permita su optimización y simplificación mediante tecnología de última generación.
Se considerarán elementos de tecnología como son equipamiento con tecnología de punta, con capacidad excedente razonablemente para permitir la escalabilidad y contener futuras compras adicionales de este tipo de activos, con elementos de tolerancia a fallas embebidos, software de virtualización y automatización para optimizar el uso de los recursos de cómputo, herramientas predictivas que nos

faciliten la gestión y reducir los tiempos de servicio en caso de incidentes o problemas y elementos de seguridad de red para cerrar puertas vulnerables y poder proteger los datos garantizando su disponibilidad e integralidad.

Asumir la gestión de su ciclo de vida mediante una estrategia sencilla, clara y lograble, conforme con las necesidades de la organización, su estructura y cultura organizacional y económicamente sostenible en el tiempo y con los recursos destinados racionalmente.
Los elementos de gestión del ciclo de vida básicos para el logro de los propósitos son los siguientes:

- Gestión de la disponibilidad
- Gestión de la salubridad
- Gestión de la remediación
- Gestión de la capacidad
- Gestión del cambio
- Gestión del servicio
- Gestión de la seguridad

Características:
Haremos una descripción lo más detallada posible, pero si tratar de sesgar selección de marcas, solamente determinando el requisito, como sigue:
Equipamiento Servidores:
Se sugiere configuraciones afinadas de acuerdo con la asignación de roles a cada uno, se escogen de manera homogénea 3 clases, los de bases de datos productivas, lo de base de datos de pruebas, ambientes de servicios y aplicaciones que requieren correr sobre servidores físicos y ambientes que permiten la virtualización.
Para los servidores que correrán las diferentes bases de datos que tienen restricciones en los términos de licenciamiento y debido a sus ediciones como son Oracle e Informix, se sugieren servidores con un solo zócalo y máximo 8 núcleos de procesamiento con la máxima frecuencia de reloj posible para explotar lo mejor posible sus capacidades, para la memoria RAM se requiere utilizar la de mayor velocidad posible que disponga de rutinas de paridad múltiples y configurada en espejo (1:1) para evitar caídas atribuibles a este delicado subsistema, deben contar también los buses PCI de última generación disponible y controladoras de red con ratas de transferencia híbrida entre 10 y 1 GbE para poder enviar tráficos con diferente prioridad, es habilitante tener doble fuente de poder y el mayor número posible sensores en elementos críticos con análisis predictivo de fallas. Dado que se utilizará una red de almacenamiento tipo SAN, se requieren controladoras tipo HBA como mínimo con capacidad de transferencia de 16Gb/seg, y con conexiones redundantes para disponer de varias rutas.
Se necesitarán servidores para ambientes de pruebas tanto de bases de datos como de aplicaciones, estos deben tener las características similares a los anteriores a excepción de la memoria RAM en arreglo, ya que esto encarece los costos y es requisito solo de cargar de trabajo productivas.
Los servidores con roles de anfitriones de virtualización para cargas de trabajo de capas de aplicación y de propósitos generales, se mantiene los requerimientos de los de bases de datos en cuanto a tolerancia a fallas, se modifica en sus capacidades de cómputo, se sugieres doble zócalo y con 16 núcleos, que con tecnología de múltiples hilos se logran hasta 32 procesadores lógicos y se optimiza el uso de las licencias de Microsoft Server como también el de los hipervisores.
Se requieren otros servidores en modo Stand Alone, corriendo algunas aplicaciones o servicios que así lo requieren, estos conservan las características de los anteriores, con menores capacidades de cómputo y sin memoria redundante.
Equipamiento sistemas de discos:
Se usarían dos tipos de sistemas, uno que presenta bloques a través de una red de almacenamiento con protocolo de fibra canal para aplicaciones muy exigentes en cuanto a latencia, se deben utilizar controladoras completamente redundantes y con la capacidad de cómputo y memoria cache suficientes, esta última con posibilidad de expansión o con la habilidad de mediante discos flash poderla expandir.

Se configurarán diferentes tipos de arreglos optimizados para cada tipo de aplicación o carga de trabajo, para los ambientes misionales en capas de bases de datos, como lo es Servinte, se sugiere la utilización de discos de estado sólido tipo Flash en arreglos de nivel 1 o espejo para garantizar el mejor tiempo de respuesta posible, con el cuidado de hacer la selección adecuada para el número de lecto/escrituras y garantizar su vida útil, para ambientes de pruebas y capas de aplicación se utilizarán discos de giros tipo SAS de velocidad media sobre arreglos que optimicen el espacio y no la transferencia, y finalmente para datos no estructurados y servicios de infraestructura que no requieran de baja latencia, se sugieren discos tipo SATA o SAS NL que hoy ofrecen grandes capacidades de almacenamiento.
Siempre las controladoras y los cajones de expansión de discos, deben disponer de doble fuente de alimentación de energía de forma redundante.
Para copias de respaldo D2D y sistemas de archivos que se ofrecen a los usuarios para la conservación de su información, se requieren sistemas tipo NAS que tienen la habilidad de presentar discos virtuales a través de la red de datos LAN, también se utilizarán para alojar grandes cantidades de archivos tipo imágenes, esto debido a que el costo ante grandes volúmenes de datos es bastante más bajo que el anterior.
Se seguirá utilizando sistemas de cintas magnéticas, se requiere un equipo que nos ofrezca características de automatización como son las librerías con varias cabezas y múltiples ranuras para el alojamiento de cintas, esto permite la zonificación y evita el intercambio manual, para el volumen de datos que se podría respaldar, se sugiere mínimo 4 unidades conectadas por fibracanal a red de almacenamiento SAN y al menos capacidad de hasta 24 cintas.
Para poder configurar las redes SAN se requieren los conmutadores, que mínimo deben tener velocidades de 16Gb/seg y puertos suficientes para conectar tantos los dispositivos de almacenamiento como los diferentes Hosts, estos elementos deben ir en esquema de redundancia para disponer de rutas alternas siempre y garantizar la disponibilidad.
Capa de virtualización:
Ya el HUV tiene experiencia con VMware, se sugiere seguir con esta tecnología en la edición más alta posible para poder optimizar el uso de los recursos y automatizar.
Para ambiente Oracle se propone como opcional virtualización con Oracle VM, de esa manera se podría optimizar el uso de costosas licencias y flexibilizar de manera importante su gestión y contingencia.
Monitorización:
Se hace obligatoria al menos para la pila de infraestructura hasta la capa de sistemas operacionales, pero esto no solamente nos debe servir para verificar la disponibilidad y salubridad, sino que nos debe apoyar la gestión de la capacidad con elementos de analítica.
Seguridad de la red:
Se sugiere seguir con la familia de UTMs que hoy manejan, pero se debe hacer cambio a una generación posterior para poder acceder a tecnologías de punta y funcionalidad enriquecida, se debe conservar el esquema de alta disponibilidad, y se hace obligatorio poder restablecer el software de medición y analítica, en lo posible subir de Analyzer a GMS.
Seguridad de los datos:
Implementar herramientas de automatización de copias de respaldo, migrando de Backup 1.0 a 2.0, esto quiere decir con la capacidad de poder realizar y mantener copias completas de los servidores tipo imagen, unificando los ambientes físicos y virtuales en una sola consola, también hacer uso de replicación para llevar a estrategia hasta protocolos de recuperación ante desastres orientados, además de los datos, a las aplicaciones y servicios corriendo. Con lo anterior también se consolida, simplifica, automatiza y controla este importante recurso, y de deja un camino expedito para la implementación de estrategias de continuidad de negocios.
Entendimiento Estratégico:
El PETI se incorpora a la organización mediante la adopción de un modelo PHVA que define las etapas de establecimiento, implementación, operación seguimiento, mantenimiento y mejora del sistema frente a la seguridad de la información.
Para el funcionamiento eficiente del El Plan Estratégico de Tecnologías de la Información, se deben identificar y relacionar todas las actividades involucradas para la protección de la información de los procesos de la organización buscando que estas prácticas de seguridad sean integradas en las labores diarias.
Esta estructura basada en procesos para la seguridad de la gestión de la información hace referencia a:

- Comprender los requisitos de seguridad de la información del UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E. y la necesidad de establecer políticas, procedimientos y objetivos en relación con la importancia de salvaguardar, proteger la integridad y confidencialidad de la información.
- Determinar, diseñar, implementar y operar controles para dar tratamiento a los riesgos de seguridad de la información del UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E. en el contexto de los riesgos que impactan los procesos de la organización.
- Incorporar actividades de protección de información a nivel de los procesos dentro del alcance del Sistema PSGI.
- Hacer y mantener un seguimiento y una revisión permanente al desempeño y a la eficacia del PETI.

- La mejora continua basada en la medición de los objetivos planteados inicialmente.
- Basado en el énfasis planteado, el Sistema Políticas de Seguridad Gestión de la Información adopta el modelo de procesos PHVA, sirviendo como base fundamental para el resto de los procesos que forman parte del sistema general del HUV:
- Planificar: Establecer la política, los objetivos, procesos y procedimientos de seguridad pertinentes para administrar el riesgo y mejorar la seguridad de la información, con el fin de entregar resultados acordes con los objetivos misionales de la organización.
- Hacer: Implementar y operar la política, los controles, procesos y procedimientos del PETI
- Verificar: Evaluar y medir el desempeño del proceso en base a la política y los objetivos de seguridad y la experiencia práctica y reportar los resultados a la alta Gerencia.
- Actuar: Realizar acciones correctivas y preventivas en base a los resultados de la auditoría interna del PSGI y la revisión por la alta Gerencia, para lograr la mejora continua del sistema.

Interrelación con otros Sistemas de Información

El Sistema de Gestión de Seguridad de la Información definido en la norma NTC-ISO/IEC 27001 y el cual es la guía básica para el diseño del PETI en el UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E. Se encuentra alineado con la NTC-ISO-IEC 27002, con el fin de apoyar la implementación y operación, consistente e integrada y garantizar la interrelación con otros sistemas de gestión relacionados que se vayan definiendo en el HUV.

Objetivo General:

Establecer medidas y patrones de administración y organización tanto de las Tecnologías de Información y Comunicaciones TIC´s, como toda la seguridad física de la información. Además de brindar los patrones necesarios para la integridad, confidencialidad y confiabilidad de la información generada por la institución.

Objetivo Específicos:

- Establecer y mantener las políticas de Seguridad de Gestión de la Información.
- Administrar los riesgos de seguridad de la información.
- Identificar y dar seguimiento a las amenazas de seguridad de la información.
- Proteger los activos de información, con base en los criterios de confidencialidad, integridad, disponibilidad.
- Fomentar y difundir las políticas de seguridad de gestión de la información, en todos los niveles del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E
- Establecer las bases fundamentales para la protección de los activos de la información ya sean físicos o electrónicos.

Alcance de la implementación y operación de las políticas de seguridad de gestión de la información

Las políticas de seguridad de gestión de la información, “PSGI”, cubren todos los aspectos administrativos, clínicos, médicos, financieros y de control que deben ser cumplidos por los directivos, funcionarios y terceros que laboren o tengan relación con el HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E, para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

El alcance de las políticas de seguridad de gestión de la Información al interior del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E, es para el proceso Gestión de Tecnología, Información y Comunicación, siendo transversal para todos los demás procesos.

Políticas de Seguridad de la Información

- Las Políticas en Informática son el conjunto de ordenamientos y lineamientos enmarcados en el ámbito jurídico y administrativo del UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E. Estas normas inciden en la adquisición y el uso de los Bienes y Servicios Informáticos al interior del Hospital HUV, las cuales se deberán de acatar invariablemente, por aquellas instancias que intervengan directa y/o indirectamente en ello.
- Las presentes políticas aquí contenidas, son de observancia para la adquisición, uso de bienes y de servicios informáticos, en el HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E. cuyo incumplimiento generará que se incurra en responsabilidad administrativa; sujetándose a lo dispuesto en la sección de políticas, políticas de cumplimiento.
- El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E deberá contar con un Jefe o responsable del Área de Sistemas, en el que recaiga la administración de los Bienes y Servicios, que vigilará la correcta aplicación de los ordenamientos.

Equipos directivos de proyectos de informática:

Están integrados por la Subgerencia de Gestión de la Información y los Jefes de Áreas o Servicios requeridos, según sea el proyecto, los cuales son responsables de:

- Velar por el funcionamiento de la tecnología informática que se utilice en las diferentes unidades administrativas.

- Elaborar y efectuar seguimiento de las implementaciones y nuevos proyectos o desarrollos.
- Definir estrategias y objetivos a corto, mediano y largo plazo.
- Controlar la calidad del servicio brindado.
- Mantener el Inventario actualizado de los recursos informáticos.

Estrategias: La estrategia informática del H.U.V. está orientada hacia los siguientes puntos:

- Plataforma de sistemas abiertos.
- Esquemas de operación bajo el concepto cliente/servidor y web en caso de desarrollos probados.
- Estandarización de hardware, software base, utilitarios y estructuras de datos.
- Intercomunicación entre unidades y equipos mediante protocolos estándares.
- Intercambio de experiencias entre departamentos de informática.
- Manejo de proyectos conjuntos con las diferentes Subgerencias.
- Programa de capacitación permanente para los colaboradores del Hospital HUV y de la Subgerencia de Gestión de la Información.
- Integración de sistemas y bases de datos del UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E.., para tener como meta final un Sistema Integral de Información Corporativo.
- Programación con ayudas visuales e interactivas. Facilitando interfaces amigables al usuario final.
- Integración de sistemas tele informáticos.
- Para la elaboración de los proyectos informáticos y de sus presupuestos, se tomarán en cuentan tanto las necesidades de hardware y software del área solicitante, como la disponibilidad de recursos con que éstas cuenten.
- La falta de conocimiento de las normas aquí descritas por parte de los colaboradores no los libera de la aplicación de sanciones y/o penalidades por el incumplimiento de las mismas.

Lineamientos para la adquisición de bienes de informática

Todo proceso de compra se rige por los procedimientos que estén vigentes por parte de la Subgerencia de Suministros. En esta política solo se presentan los lineamientos de definición técnica de la Subgerencia de Gestión de la Información.

Toda adquisición de tecnología informática de impacto se efectúa a través de la Subgerencia de Gestión de la Información, con el visto bueno de la Gerencia General para casos menores como Software de bajo valor, PC´s aislados, portátiles, impresoras o dispositivos por unidad, se efectúa por un grupo conformado por el Subgerente de Gestión de la Información y el Jefe del Área o Servicio solicitante de bienes o servicios informáticos, con la aprobación de la Gerencia General.

La Subgerencia de Gestión de la Información, al planear las operaciones relativas a la adquisición de bienes informáticos, establecerá prioridades y en su selección deberá tener en cuenta:

- Precio: Costo inicial, costo de mantenimiento y consumibles por el período estimado de uso de los equipos.
- Calidad: Parámetro cualitativo que especifica las características técnicas de los recursos informáticos.
- Experiencia: Presencia en el mercado nacional e internacional, estructura de servicio, la confiabilidad de los bienes y certificados de calidad con los que se cuente.
- Desarrollo Tecnológico: Se deberá analizar su grado de obsolescencia, su nivel tecnológico con respecto a la oferta existente y su permanencia en el mercado.
- Estándares: Toda adquisición se basa en los estándares, es decir la arquitectura del H.U.V. establecida por el Comité. Esta arquitectura tiene una permanencia mínima de dos a cinco años.
- Capacidades: Se deberá analizar si satisface la demanda actual con un margen de holgura y capacidad de crecimiento para soportar la carga de trabajo del área.

Para la adquisición de Hardware se observará lo siguiente:

- El equipo que se desee adquirir deberá estar dentro de las listas de ventas vigentes de los fabricantes y/o distribuidores del mismo y dentro de los estándares que defina la Subgerencia de Suministros del HUV.
- Deberán tener un año de garantía como mínimo.
- Deberán ser equipos integrados de fábrica o ensamblados con componentes previamente evaluados por esta Subgerencia.
- La marca de los equipos o componentes deberá contar con presencia y permanencia demostrada en el mercado nacional e internacional, así como con asistencia técnica y soporte técnico local.
- Tratándose de equipos microcomputadoras, a fin de mantener actualizado la arquitectura informática del UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E.., la Subgerencia de Gestión de la Información emitirá las especificaciones técnicas mínimas para su adquisición, cuando la Subgerencia de Suministros del HUV, lo solicite.
- Los dispositivos de almacenamiento, así como las interfaces de entrada/salida, deberán estar acordes con la tecnología de punta vigente, tanto en velocidad de transferencia de datos, como en el ciclo del proceso.

- Las impresoras deberán apegarse a los estándares de hardware y software vigentes en el mercado y del UNIVERSITARIO DEL VALLE “EVARISTO GARCÍA” E.S.E.., corroborando que los suministros (tóneres, papel, etc.) se consigan fácilmente en el mercado y no estén sujetas a un solo proveedor.
- Conjuntamente con los equipos, se deberá adquirir (para los casos requeridos) el equipo complementario adecuado para su correcto funcionamiento de acuerdo con las especificaciones de los fabricantes, y que esta adquisición se manifieste en el costo de la partida inicial.
- Los equipos complementarios deberán tener una garantía mínima de un año y deberán contar con el servicio técnico correspondiente en la región.
- Los equipos adquiridos deben contar de preferencia, con asistencia técnica durante la instalación de los mismos.
- En lo que se refiere a los computadores denominados servidores, equipo de comunicaciones como switches, routers, y otros que se justifiquen por ser de operación crítica y/o de alto costo; al vencer su período de garantía, deben de contar con un programa de mantenimiento preventivo y correctivo que incluya el suministro de partes o repuestos.
- En lo que se refiere a los computadores denominados personales, al vencer su garantía por adquisición, deben de contar por lo menos con un programa de servicio de mantenimiento correctivo que incluya el suministro de partes o repuestos.

En la adquisición de equipos de cómputo si se requiere incluir software pre-instalado, éste debe de ser vigente y con su licencia correspondiente.
En términos generales, sólo se adquirirán las últimas versiones liberadas de los productos seleccionados, salvo situaciones específicas que se deberán justificar ante la Subgerencia de Gestión de la Información.
Todos los productos de Software que se adquieran deberán contar con su licencia de uso, documentación y garantía respectivos.
Todos los productos de software que se utilicen a partir de la fecha en que entre en vigor el presente documento, deberán contar con su licencia de uso respectiva; por lo que se promoverá la regularización o eliminación de los productos ya instalados que no cuenten con la licencia respectiva.
Todo el software utilizado por colaboradores como contratistas y empleados del hospital deberá estar correctamente licenciado y será el titular de la licencia o dueño del equipo de cómputo quien sea responsable por el uso de la misma. En caso que el funcionario o contratistas requiera utilizar software para ejecutar tareas propias del hospital, utilizando software con titularidad personal, deberá informar a la Subgerencia de Gestión de la Información para proveer el licenciamiento adicional necesario para ejecutar dichas actividades.
Cuando el Hospital contrata o conviene actividades y servicios con otra institución, el software que empleen los contratistas para las actividades relacionadas en el contrato, deberá estar correctamente licenciado y será la organización contratada quien verifique y certifique la propiedad del software.
Todo proyecto de contratación de desarrollo o construcción de software requiere de un estudio de factibilidad que permita establecer la rentabilidad del proyecto así como los beneficios que se obtendrán del mismo.
8.8 Gestión de información
Objetivo:
Brindar a los funcionarios del Hospital Universitario del Valle “Evaristo García” E.S., que tienen bajo su responsabilidad la clasificación de la información, un instrumento para determinar el nivel de criticidad y el valor de la información, con el fin de identificar los controles de seguridad requeridos para salvaguardarla adecuadamente, así como los controles y autorización de acceso por parte de los funcionarios y terceras personas que apoyan las actividades del Hospital HUV.
Alcance: Se aplica a todos los procesos de la institución.
Definiciones:
Titular de la información: Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.
Usuario: El usuario es la persona natural o jurídica que, en los términos y circunstancias previstos, puede acceder a información personal de uno o varios titulares de la información suministrada por el operador o por la fuente, o directamente por el titular de la información. El usuario, en cuanto tiene acceso a información personal de terceros, se sujeta al cumplimiento de los deberes y responsabilidades previstos para garantizar la protección de los derechos del titular de los datos.
Dato personal: Es cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica. Los datos personales pueden ser públicos, semiprivados o privados.
Dato público: Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la presente ley. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas.
Dato semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o

a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
Dato privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
Datos personales sensibles: se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.
Información: Hace referencia a los datos tratados que se encuentran en forma digital o no digital Se empleará como base para esta metodología la definición de la familia de normas ISO 27000 y la Información en forma digital o no digital creada, procesada, almacenada, archivada o borrada durante la ejecución de procesos misionales; por ejemplo: Bases de datos, registros, correos electrónicos, código fuente, documentos en papel, diseños, datos procesados, listas de contactos, calendarios, imágenes y toda aquella información que se considere con valor para el Hospital HUV.
Por otra parte, la ley 1712/2014, la define como: “Un conjunto organizado de datos contenido en cualquier documento que los sujetos obligados generen, obtengan, adquieran, transformen o controlen”.
Información pública reservada: De acuerdo a la ley 1712/2014 se define como: “Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley”.
Información pública clasificada: De acuerdo a la ley 1712/2014 se define como: “Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley”.
Información privada: La jurisprudencia de la Corte Constitucional, en Sentencia T-729 de 2002, hace referencia a la información privada de la siguiente manera:
“La información privada, será aquella que por versar sobre información personal o no, y que por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio “.
Responsabilidad: Titular de la Información.

- Actualizar y rectificar sus datos personales frente al Responsable del Tratamiento o Encargados del Tratamiento, cuando sea necesario.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 y las demás normas que la modifiquen, adicionen o complementen.
- Revocar la autorización y/o solicitar la supresión del dato, cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales.
- Responsable del Tratamiento.
- Decidir sobre las bases de datos y/o el tratamiento de los datos.
- Dar a conocer, actualizar y rectificar los datos personales de los titulares de acuerdo con los requerimientos de los mismos.
- Entregar las pruebas de la autorización otorgada por el titular de los datos, salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el Artículo 10 de la Ley 1581 de 2012.
- Informar al propietario de la información del tratamiento de sus datos personales, previa solicitud.
- Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Solicitar y conservar, en las condiciones previstas en la Ley 1581 de 2012, copia de la respectiva autorización otorgada por el titular.
- Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información que se suministre al encargado del tratamiento sea verás, completa, exacta, actualizada, comprobable y comprensible.
- Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a éste se mantenga actualizada.
- Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.
- Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la Ley 1581 de 2012.
- Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.

- Tramitar las consultas y reclamos formulados, en los términos señalados en la Ley 1581 de 2012.
- Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- Informar a solicitud del titular sobre el uso dado a sus datos.
- Informar a la autoridad de protección de datos, cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
- Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

Responsable de la producción de la información

- Tiene responsabilidad aprobada por el nivel directivo del HOSPITAL HUV para controlar la generación, clasificación, desarrollo, mantenimiento, uso y protección adecuada de la información.
- Identificar todas las fuentes de información, concientizar a sus funcionarios sobre la importancia de la clasificación de la información para la adecuada operación del HOSPITAL HUV.
- Asegurar que se cumplan los controles para preservar la confidencialidad, la integridad y la disponibilidad de la información.
- Tomar decisiones esenciales de costo beneficio para lograr el cumplimiento de los objetivos de la entidad.
- Mantener un nivel apropiado de protección física y lógica sobre la información.
- Revisar periódicamente la clasificación de la información.
- Asegurar la disponibilidad de la información en todo momento.
- Revisar periódicamente la efectividad de los controles sobre la información.
- Definir y revisar periódicamente las restricciones de acceso y niveles de clasificación de la información, considerando las políticas definidas por el Comité de Sistemas del HOSPITAL HUV.
- Determinar y revisar periódicamente el esquema de respaldo y restauración de la información.

Encargado del Tratamiento.

- Tiene la responsabilidad de tratar los datos personales sobre las bases de datos y/o fuentes de información.
- Dar a conocer, actualizar y rectificar los datos personales de los titulares de acuerdo con los requerimientos de los mismos y lo indicado por el responsable del tratamiento.
- Informar al propietario de la información del tratamiento de sus datos personales previa solicitud, de acuerdo con lo indicado por el responsable del tratamiento.
- Garantizar al titular, en todo tiempo el pleno y efectivo ejercicio del derecho de hábeas data.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Realizar oportunamente la actualización, rectificación o supresión de los datos personales en los términos de la Ley 1581 de 2012.
- Actualizar la información reportada por los responsables del tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
- Tramitar las consultas y los reclamos sobre datos personales formulados por los titulares en los Términos señalados en la Ley 1581 de 2012
- Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la Ley 1581 de 2012.
- Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
- Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
- Permitir el acceso a la información, únicamente a las personas que pueden tener acceso a ella de acuerdo con los procedimientos establecidos
- Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.

Consultado.

- Verificar los niveles, categorías o tipos de clasificación de la información y sus actualizaciones.
- Definir los criterios para la clasificación de la información y los procedimientos de manejo en conjunto con los propietarios de la información.
- Decidir sobre casos en los que se tengan dudas sobre la clasificación de un cierto tipo de información.
- Apoyar a los Propietarios de la Información en la determinación de los requerimientos de protección y mecanismos de control de cada categoría de clasificación.

Informado.

- Conocer los tipos de clasificación de la información y las normas concernientes a él.
- Divulgar y aplicar las normas de clasificación de la información establecidas por el HOSPITAL HUV.
- Responsable de la Información.
- Responsable de proteger la información, manteniendo los controles definidos por el dueño de la información.
- Obtener aprobación del propietario de la información antes de realizar la divulgación de la misma.
- Realizar y aprobar las copias de respaldo de la información para garantizar su disponibilidad.
- Realizar restauraciones de las copias de respaldo.
- Implementar los controles de acceso definidos o aprobados por el propietario de la información.
- Realizar las tareas administrativas propias de su cargo con la información bajo su custodia.

Usuario Final (Funcionarios HOSPITAL HUV).

- Recibir y dar un buen uso al activo de información asignado.
- Orientar a los jefes de dependencia en la clasificación de la información.
- Garantizar la confidencialidad de la información que conoce, de acuerdo a sus responsabilidades y funciones.
- Firmar las actas y documentos relacionados con los activos de información.
- Colaborar con los jefes de dependencia a mantener actualizada la matriz de activos de información, las aplicaciones asociadas y la clasificación de la información a su cargo.
- Contribuir con la disposición final de la información, acorde con el manual de gestión de correspondencia y archivos oficiales y con las Tablas de Retención Documental.

GENERALIDADES
Las áreas del HOSPITAL HUV deberán clasificar su información de acuerdo a su valor y criticidad. Esta clasificación debe realizarse de acuerdo a las necesidades que tiene el área de compartir o restringir la información, los requerimientos de seguridad en términos de confidencialidad, integridad y disponibilidad, y con base al impacto que pudiera provocar en términos económicos, operativos, legales e imagen institucional.
El dueño o propietario de la información, será el responsable de definir la categoría en la que cada activo de información se encuentra, así como determinar si es necesario un proceso de reclasificación y los controles requeridos para su protección.
Para la clasificación de la información el HOSPITAL HUV adoptará el siguiente esquema:

- Pública: El HOSPITAL HUV establece que la información pública es aquella que ha sido declarado de conocimiento público por parte de la persona con autoridad para hacerlo o por alguna norma jurídica. Esta información puede ser entregada o publicada sin restricciones a terceros, funcionarios o cualquier persona sin ocasionar daños a terceros ni a los procesos de negocio del HOSPITAL HUV.
- Confidencial: El HOSPITAL HUV establece que la información confidencial es toda aquella que no es pública. Y a la información pública solo pueden tener acceso las personas que han sido declaradas usuarios legítimos de esta información con privilegios asignados, como se expresa en los activos de información.

Los niveles de confidencialidad de los activos de información del HOSPITAL HUV son los siguientes:

- Uso Interno: Es la información que es utilizada por el HOSPITAL HUV para realizar sus labores en los procesos y que no puede ser utilizada por terceros sin autorización del propietario del activo de información. En caso de ser conocida, utilizada o modificada por personas no autorizadas impactaría de manera leve a los procesos de la entidad.
- Restringida: Información que es utilizada por solo un grupo de funcionarios del HOSPITAL HUV para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin previa autorización del propietario del activo de información. En caso de ser conocida, utilizada o modificada por personas no autorizadas impactaría de manera importante a los procesos de la entidad.
- Altamente Restringida: Información que es utilizada por solo un grupo de funcionarios del HOSPITAL HUV para realizar sus labores y que no puede ser conocida por otros funcionarios o terceros sin previa autorización del HOSPITAL HUV. En caso de ser conocida, utilizada o modificada por personas no autorizadas impactaría de manera grave a los procesos de la entidad.
- Toda la información que se maneja dentro de cada una de las Áreas tendrá carácter de CONFIDENCIAL hasta que se apruebe otro tipo de clasificación.

Etiquetado y manejo de la información:

- Los documentos con información del tipo “restringida” deberán ser controlados por medio de copias individuales perfectamente numeradas y registro de las personas que han tenido acceso.
- La copia o transferencia de información “restringida” por cualquier medio (electrónico, magnético, en papel) deberá estar autorizada y controlada.

- Todos los documentos del tipo “Altamente Restringida” se deberán conservar bajo llave y en lugares seguros.
- El envío de documentos con clasificación Confidencial (De Uso Interno, Restringida y Altamente Restringido), se deberá hacer por medio de canales seguros tales como mensajería privada, correo electrónico cifrado o entrega personal. En caso de hacerse por medio de forma física, los paquetes deberán estar debidamente cerrados y que sea imposible observar su contenido.
- Toda recepción de información confidencial deberá solicitar acuse de recibo.
- En caso de ser necesario, se considerará un procedimiento o centro de destrucción de documentos y activos de información que garantice la no reutilización de la información. La destrucción de registros e información del HOSPITAL HUV debe ser formalmente autorizada por el responsable.
- La información Confidencial (De Uso Interno, Restringida y Altamente Restringido) deberá reflejar por medio de una leyenda, la clasificación a la que pertenece, sin importar la forma o medio en la que se encuentre para ello se debe tener en cuenta la ilustración del punto 5.3.
- El HOSPITAL HUV, a través de sus instancias correspondientes, se reserva el derecho de iniciar denuncias, y procesos disciplinarios para sancionar a los funcionarios que divulguen o destruyan ilícitamente la información de la entidad.

Se deben tener en cuenta los siguientes lineamientos o controles para el manejo y transporte de información confidencial.

- Política de control de acceso a la información
- Proceso Disciplinario
- Propiedad de los activos
- Devolución de Activos
- Clasificación de la información
- Etiquetado de la información
- Manejo de Activos
- Transferencia de medios físicos

NORMATIVIDAD

TIPO	**NUMERO**	**NOMBRE**	**FECHA**
Ley	712	Ley de Transparencia y Acceso a la Información Pública Objeto. El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.	6 Marzo / 2014
Ley	1266	Ley Habeas Data La cual “dicta disposiciones generales del Habeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países”	31 Dic. / 2008
Ley	1581	Ley de Protección de Datos Por la cual se desarrolla el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.	31 Oct / 2012

Seguridad en la Red de Datos

Introducción

La información es una herramienta útil en la toma de decisiones de una organización, por su valor incalculable, es necesario protegerla. Con el avance de la tecnología que cada día se perfecciona, específicamente en el campo de las comunicaciones y con la capacidad del computador para comunicarse con otros dispositivos remotos y para comunicar entre si computadores físicamente separados en los que llamamos una red de transmisión de datos, la cual es importante en el diseño de muchos sistemas de información. Pero esta información si no está debidamente protegida cuando se realiza el proceso de transmisión de datos puede generar pérdidas costosas e importantes a diversas organizaciones, lo que generaría riesgos e incertidumbre en la exactitud de la información, por esto es muy importante desarrollar políticas de seguridad claras con la intención de mantener seguros los datos durante el proceso de emisión, transporte y recepción.

Seguridad de la información en la Red

Se puede entender la seguridad como la necesidad de proteger. En una red se deben proteger todos los

equipos que posibilitan el proceso de la comunicación, las personas que producen, acceden y distribuyen los datos y finalmente la información que es considerada como uno de los activos más importantes de las organizaciones.
Para mantener segura la información que viaja a través de la red esta debe cumplir con tres requisitos:

- Integridad: Requiere que los recursos sean modificados por quienes están autorizados y que los métodos y los procesamientos de la información sean salvaguardados en su totalidad y con exactitud.
- Confidencialidad: Se debe garantizar que la información sea accesible solo por quienes están autorizados para su lectura, cambios, impresión y formas de revelación
- Disponibilidad: Se requiere que la información esté disponible en el momento exacto para quienes están autorizados a acceder a ella.

Ataques a la seguridad de la red
Dentro del proceso de comunicación existen dos tipos de ataques a la red de transmisión de datos a saber:

- Ataques pasivos: Son oidores o monitoreo de las transmisiones. El objetivo de quienes realizan ese tipo de ataque es obtener la información que se está transmitiendo. En este tipo de ataque se pueden encontrar:
- Divulgación del contenido de un mensaje: es un tipo de ataque pasivo por medio del cual el atacante se entera de la información transmitida; como por ejemplo escuchar una llamada telefónica, leer un correo electrónico abierto.
- Análisis de Tráfico: Este tipo de ataque pasivo se realiza cuando el atacante puede determinar la localización e identidad de quienes se están comunicando y determinar el mensaje que está siendo transmitido aun cuando esté protegido por medio de cifrado.
- Ataques activos: Suponen modificación de los datos o creación de flujos de datos falsos. Dentro de este tipo de ataques se pueden encontrar.

Norma ISO 17799

- Enmascaramiento: Es un tipo de ataque activo que tiene lugar cuando una entidad pretende suplantar a otra para obtener información confidencial.
- Repetición: Se realiza con la captura de unidades de datos que se vuelven a retransmitir para producir efectos no autorizados.
- Modificación de Mensajes: Se modifican los mensajes para producir efectos no autorizados.
- Denegación de Servicios: Previene o inhabilita el uso normal de las facilidades de comunicación, usualmente se hace para obtener un fin específico o para obtener perturbaciones sobre la red desmejorando su rendimiento o incluso inhabilitando la misma.

Herramientas de seguridad

Existen métodos o herramientas tecnológicas que ayudan a las organizaciones a mantener segura la red. Estos métodos, su utilización, configuración y manejo dependen de los requerimientos que tenga la organización para mantener la red en un funcionamiento óptimo y protegido contra los diferentes riesgos. Los más utilizados son:

Autenticación: Identifica quien solicita los servicios en una red. Esta no hace referencia solo a los usuarios sino también a la verificación de un proceso de software.

Autorización: Indica que es lo que un usuario puede hacer o no cuando ingresa a los servicios o recursos de la red. La autorización otorga o restringe privilegios a los procesos y a los usuarios.

Auditoria: Para analizar la seguridad de una red y responder a los incidentes de seguridad, es necesario hacer una recopilación de datos de las diferentes actividades que se realizan en la red, a esto se le llama contabilidad o auditoria. Con normas de seguridad estrictas la auditoria debe incluir una bitácora de todos los intentos que realiza un usuario para lograr conseguir la autenticación y autorización para ingresar a la red. También debe registrarse los accesos anónimos o invitados a los servidores públicos, así como registrar los intentos de los usuarios para cambiar sus privilegios.
Cifrado: Es un proceso que mezcla los datos para protegerlos de su lectura, por parte de otro que no sea el receptor esperado. Un dispositivo de cifrado encripta los datos colocándolos en una red. Esta herramienta constituye una opción de seguridad muy útil, ya que proporciona confidencialidad a los datos. Se recomienda el cifrado de datos en organizaciones cuyas redes se conectan a sitios privados a través de Internet mediante redes privadas virtuales.
Filtros de paquete: Se pueden configurar en routers o servidores para rechazar paquetes de direcciones o servicios concretos. Los filtros de paquete ayudan a proteger recursos de la red del uso no autorizado, destrucción, sustracción y de ataques de denegación del servicio. Las normas de seguridad deben declarar si los filtros implementan una de las siguientes normas:

- Denegar tipos específicos de paquetes y aceptar todo lo demás
- Aceptar tipos específicos de paquetes y denegar todo lo demás.

Firewalls: Es un sistema o combinación de sistemas, que exige normas de seguridad en la frontera entre dos o más redes.
Vlan: En una red LAN se utilizan los switches para agrupar estaciones de trabajo y servidores en agrupaciones lógicas.
En las redes, las VLAN se usan para que un conjunto de usuarios en particular se encuentre agrupado lógicamente.
Las VLAN permiten proteger a la red de potenciales problemas conservando todos los beneficios de rendimiento.
Detección de Intrusos: Una intrusión es cualquier conjunto de acciones que puede comprometer la integridad, confidencialidad o disponibilidad de una información o un recurso informático. Los intrusos pueden utilizar debilidades en la arquitectura de los sistemas y el conocimiento interno del sistema operativo para superar el proceso normal de autenticación. Una intrusión significa:

- Acceder a una determinada información.
- Manipular cierta información.
- Hacer que el sistema no funcione de forma segura o inutilizarlo.
- Un routers (enrutador) es un dispositivo hardware o software de interconexión de redes de computadores que opera en la capa tres (nivel de red) del modelo OSI.
- Un firewall (cortafuegos), es un elemento de hardware o software utilizado en una red de computadores para prevenir algunos tipos de comunicaciones prohibidos según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red.
- Un switche (conmutador) es un dispositivo de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI.

Seguridad de redes: Es un nivel de seguridad que garantiza que el funcionamiento de todas las máquinas de una red sea óptimo y que todos los usuarios de estas máquinas posean los derechos que les han sido concedidos:
Esto puede incluir:

- Evitar que personas no
- autorizadas intervengan en el sistema con fines malignos
- Evitar que los usuarios realicen operaciones involuntarias que puedan dañar el sistema
- Asegurar los datos mediante la previsión de fallas
- Garantizar que no se interrumpan los servicios

Las causas de inseguridad: Generalmente, la inseguridad puede dividirse en dos categorías:

- Estado de inseguridad activo: es decir, la falta de conocimiento del usuario acerca de las funciones del sistema, algunas de las cuales pueden ser dañinas para el sistema (por ejemplo, no desactivar los servicios de red que el usuario no necesita).
- Estado pasivo de inseguridad: es decir, cuando el administrador (o el usuario) de un sistema no está familiarizado con los mecanismos de seguridad presentes en el sistema.

El objetivo de los atacantes (también denominados "piratas" o "hackers"):

- La atracción hacia lo prohibido
- El deseo de obtener dinero (por ejemplo, violando el sistema de un banco)
- La reputación (impresionar a sus amigos)
- El deseo de hacer daño (destruir datos, hacer que un sistema no funcione)

El comportamiento del atacante: Frecuentemente, el objetivo de los atacantes es controlar una máquina para poder llevar a cabo acciones deseadas. Existen varias formas de lograr esto:

- Obteniendo información que puede utilizarse en ataques
- Explotando las vulnerabilidades del sistema
- Forzando un sistema para irrumpir en él

¿Cómo es posible protegerse?

- Manténganse informado
- Conozca su sistema operativo
- Limite el acceso a la red (firewall)
- Limite el número de puntos de entrada (puertos)
- Defina una política de seguridad interna (contraseñas, activación de archivos ejecutables)
- Haga uso de utilidades de seguridad (registro)

Políticas de Seguridad de la Red
Política de uso de puntos de red de datos (Red de Área Local – LAN).
Objetivo: Asegurar la operación correcta y segura de los puntos de red.
Aplicabilidad: Estas son políticas que aplican todos los procesos del Hospital HUV.
Directrices:

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos estándar.
- Los equipos de uso personal, que no son de propiedad del HOSPITAL HUV, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el Área de la Subgerencia de Gestión de la Información del HOSPITAL HUV.
- La instalación, activación y gestión de los puntos de red es responsabilidad de la Subgerencia de Gestión de la Información.

Políticas de seguridad del centro de datos y centros de cableado
Objetivo: Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.
Aplicabilidad: Estas políticas aplican a los funcionarios, contratistas, colaboradores del HOSPITAL HUV actuales o por ingresar y a terceros que estén encargados de cualquier parte o sistema de la plataforma informática, Data Center.
Directrices:

- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.
- El Área de Información y Sistemas debe garantizar que el control de acceso al centro de datos del HOSPITAL HUV, cuenta con dispositivos electrónicos de autenticación o sistema de control biométrico.
- La Subgerencia de Gestión de la Información deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía.
- La limpieza y aseo del centro de datos estará a cargo del Área Administrativa y debe efectuarse en presencia de un funcionario de la Subgerencia de Gestión de la Información del HOSPITAL HUV.
- El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.

En las instalaciones del centro de datos o centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales que representen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.
El centro de datos debe estar provisto de:

- Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
- Pisos elaborados con materiales no combustibles.
- Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
- Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una falla momentánea del fluido eléctrico de la red pública.
- Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- La grabación de vídeo en las instalaciones del centro de datos debe estar expresamente autorizada por el Comité de Seguridad Informática y de Sistemas y exclusivamente con fines institucionales.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario o contratista autorizado del HOSPITAL HUV.
- Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere

ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.
- Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.
- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

Políticas de seguridad de los Equipos
Objetivo: Asegurar la protección de la información en los equipos.
Aplicabilidad: Estas son políticas que aplican todos los procesos del Hospital HUV.
Directrices:

- Protecciones en el suministro de energía: A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada. Esta labor debe ser revisada por el área Administrativa.
- Seguridad del cableado: Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
- Deben existir planos que describan las conexiones del cableado.
- El acceso a los centros de cableado (Racks), debe estar protegido.
- Mantenimiento de los Equipos: El HOSPITAL HUV debe mantener contratos de soporte y mantenimiento de los equipos críticos.
- Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.
- Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.
- Los equipos que requieran salir de las instalaciones del HOSPITAL HUV para reparación o mantenimiento, deben estar debidamente autorizados y se debe garantizar que en dichos elementos no se encuentra información establecida como crítica en la clasificación de la información de acuerdo a los niveles de clasificación de la información.
- Para que los equipos puedan salir fuera de las instalaciones, se debe suministrar un nivel mínimo de seguridad, que al menos cumpla con los requerimientos internos, teniendo en cuenta los diferentes riesgos de trabajar en un ambiente que no cuenta con las protecciones ofrecidas en el interior del HOSPITAL HUV.
- Cuando un dispositivo vaya a ser reasignado o retirado de servicio, debe garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información, utilizando herramientas para realizar sobre-escrituras sobre la información existente o la presencia de campos magnéticos de alta intensidad. Este proceso puede además incluir, una vez realizado el proceso anterior, la destrucción física del medio, utilizando impacto, fuerzas o condiciones extremas.

Ingreso y retiro de activos de información de terceros.

- El retiro e ingreso de todo activo de información de propiedad de los usuarios del HOSPITAL HUV, utilizados para fines personales, se realizará mediante los procedimientos establecidos por la Administración del Edificio.
- El HOSPITAL HUV no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica del Departamento.
- El retiro e ingreso de todo activo de información de los visitantes que presten servicios al HOSPITAL HUV (consultores, pasantes, visitantes, etc.) será registrado y controlado en las porterías del edificio. El personal de vigilancia de recepción verificará y registrará las características de identificación del activo de información.
- El traslado entre dependencias del HOSPITAL HUV de todo activo de información, está a cargo del área Administrativa, para el control de inventarios.

Política de establecimiento, uso y protección de claves de acceso.
Objetivo: Controlar el acceso a la información.
Aplicabilidad: Estas son políticas que aplican todos los procesos del Hospital HUV.
Directrices:

- Se debe concienciar y controlar que los usuarios sigan buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.
- Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le signen para la utilización de los equipos o servicios informáticos de la Entidad.

- Los usuarios deben tener en cuenta los siguientes aspectos:
- No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.
- El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato.
- Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.
- Se bloqueará el acceso a todo usuario que haya intentado el ingreso, sin éxito, a un equipo o sistema informático, en forma consecutiva por cinco veces.
- La clave de acceso será desbloqueada sólo por el PUC (Punto Único de Contacto, luego de la solicitud formal por parte del responsable de la cuenta. Para todas las cuentas especiales, la reactivación debe ser documentada y comunicada al PUC.
- Las claves o contraseñas deben: Poseer algún grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
- Tener mínimo diez caracteres alfanuméricos.
- Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema.
- Cambiarse obligatoriamente cada 30 días, o cuando lo establezca el Área de la Subgerencia de Gestión de la Información.
- Cada vez que se cambien estas deben ser distintas por lo menos de las últimas tres anteriores.
- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni todos alfabéticos.
- No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
- No ser reveladas a ninguna persona, incluyendo al personal del Área de Información y Sistemas.
- No regístralas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

El Hospital Universitario del Valle “Evaristo García” E.S.E “Evaristo García” E.S.E “Evaristo García” ESE, en cumplimiento de lo dispuesto por la Ley 1581 de 2012 y el Decreto 1377 de 2013 que regulan la recolección y tratamiento de los datos de carácter personal, y establece las garantías legales que deben cumplir todas las personas en Colombia para el debido tratamiento de la información, expide la siguiente norma que desarrolla la política de seguridad de la información para el manejo y preservación de datos personales dentro de la entidad.
Definición de Términos:
Subgerencia Gestión de la Información: servicio responsable y que gestiona la Red de datos del HOSPITAL HUV.
Red de datos del HOSPITAL HUV: red de comunicaciones que conecta todos los ordenadores y dispositivos de red del HOSPITAL HUV entre ellos y con Internet.
Usuarios de la Red de datos del HOSPITAL HUV: estudiantes, profesores, investigadores, personal, usuarios de las instituciones conectadas y en general cualquier persona que por su relación con el HOSPITAL HUV tenga derecho a usar la Red de datos.
Normas de Uso Aceptable y Seguridad: documento que recoge la normativa orientada a lograr el uso correcto y seguro de una red en un determinado ámbito.
Instituciones conectadas a través de la red de datos del HOSPITAL HUV: toda institución que se encuentre directamente conectada a la red de datos del HOSPITAL HUV.
Introducción: La Red de datos del HOSPITAL HUV conecta los ordenadores y otros dispositivos susceptibles de ser conectados dentro de su plataforma entre ellos y con otras redes de investigación y comerciales como por ejemplo Internet.
La finalidad de esta interconexión es dotar a los usuarios de la red de los medios necesarios para la realización de las tareas investigadora, docente y administrativa.
Subgerencia Gestión de la Información, previa petición del usuario, proporciona conexión a la Red de Datos del HOSPITAL HUV y a los servicios que en ella se ofrecen como pueden ser, correo electrónico, acceso a internet, etc.
El uso de la Red de datos del HOSPITAL HUV deberá:

- Respetar los fines para los que ha sido creada.
- Evitar la interrupción de los servicios que ofrece o de otros equipos que forman parte de la infraestructura de la Red de datos del HOSPITAL HUV
- Evitar interferencias e interrupciones en el trabajo de otros usuarios de la Red de datos del HOSPITAL HUV
- Evitar situaciones que afecten a la seguridad de la Red de datos del HOSPITAL HUV y a sus usuarios.
- Respetar el contenido de las leyes y demás disposiciones normativas y legales a nivel nacional.
- Respetar dentro del campus del HOSPITAL HUV el rango de radiofrecuencias entre los 2.4 y 5 GHz para uso de la red inalámbrica

Ámbito de aplicación: Las normas contenidas en este documento serán de aplicación a todos los usuarios

e instituciones de la red de datos del HOSPITAL HUV en tanto en cuanto hagan uso de la red y de los servicios ofrecidos.
Las instituciones conectadas a la red de datos del HOSPITAL HUV deben tener sus propias Normas de uso y seguridad de la red dentro del contexto de los servicios que ofrece a sus usuarios. Dichas Normas deberán ser compatibles con las condiciones y términos expresados en el presente documento.
Los usuarios e instituciones serán informados de estas Normas de Uso Aceptable y Seguridad y aceptan que la Oficina Coordinadora de Gestión de la Información sea el ente, responsable del cumplimiento de las mismas.
La Oficina Coordinadora de Gestión de la Información podrá proponer al Consejo de Administración del HOSPITAL HUV modificaciones a este documento para ajustarlo a la lógica evolución tecnológica y legislativa que se produzca, manteniendo el espíritu del mismo en lo que respecta a los objetivos y finalidades para los que se creó la red y que se describen en el punto de Seguridad de la información en la Red. Los usuarios e instituciones serán puntualmente informados de cualquier modificación que fuera preciso introducir.
Términos y condiciones: Para garantizar y optimizar el funcionamiento de la Red de Datos del HOSPITAL HUV, es necesaria una serie de compromisos entre los usuarios y los responsables de la red.
La Oficina Coordinadora de Gestión de la Información debe asegurar:

- Conectividad a la Red de Datos del HOSPITAL HUV a todos los usuarios de la institución, cumpliendo siempre con las normas de uso y seguridad.
- Acceso a los servicios que están detallados en el Catálogo de Servicios ofrecidos por Oficina Coordinadora de Gestión de la Información en los términos recogidos en el mismo.
- La salvaguardia del espectro de radiofrecuencias entre 2.4 y 5 GHz que utiliza la red inalámbrica.

Los compromisos por parte de los usuarios de la Red de Datos del HOSPITAL HUV son los siguientes:

- Hacer buen uso de la Red de datos institucional.
- No interferir con el espectro de radiofrecuencias entre 2.4 y 5 GHz que utiliza la red inalámbrica.
- Cumplir las normas de seguridad definidas en el punto de Seguridad de la información en la Red.
- No utilizar su conexión a la Red de datos del HOSPITAL HUV para proporcionar tráfico a terceras personas o entidades, salvo por expreso consentimiento de los organismos responsables de la red.
- No solicitar más recursos de los que a corto o medio plazo vayan a ser utilizados.
- Comunicar los problemas que surjan al HelpDesk de la Oficina Coordinadora de Gestión de la Información para su resolución.
- Utilizar correctamente los recursos que se le suministran.

Normas de seguridad: La conexión de un ordenador a la Red de datos del HOSPITAL HUV conlleva ciertos riesgos desde el momento en que dicho equipo se conecte a Internet.
Desde Internet llegan diariamente ataques, virus, gusanos, etc., y para minimizar los riesgos los usuarios del HOSPITAL HUV deben cumplir las siguientes normas de seguridad:

- Todo computador o dispositivo móvil conectado a la red del HOSPITAL HUV deberá estar protegido por una contraseña suficientemente robusta, es decir, no trivial o evidente.
- Deben aplicarse periódicamente todas las actualizaciones de seguridad para el sistema operativo que esté usando. Esta tarea es fácilmente automatizable en la mayoría de los casos.
- Si su sistema operativo es Windows o Macintosh, debe instalarse el antivirus institucional proporcionado por el Hospital HUV.
- No compartir carpetas sin contraseña.

Además de las anteriores normas, se recomienda:

- Instalar solo el software que vaya a necesitar.
- En la medida de lo posible sustituir los protocolos que no encriptan las contraseñas por otros que si las encripten. Por ejemplo, si se usa telnet, sustituirlo por ssh.
- No instalar servicios de red que no se vayan a usar.

Uso aceptable: Los usuarios de la Red de datos del HOSPITAL HUV utilizarán la infraestructura de la red de esta institución para el intercambio de información cuyo contenido sea de investigación, académico, educacional o necesario para el desempeño de la función administrativa.
Los usuarios de la Red de datos del HOSPITAL HUV deberán utilizar eficientemente la red con el fin de evitar, en la medida de lo posible, la congestión de la misma.
Uso no aceptable: La infraestructura y servicios ofrecidos por la red de datos del HOSPITAL HUV no deben usarse para:

- Cualquier transmisión de información o acto que viole la legislación vigente.
- Fines privados, personales o lúdicos (Juegos, música, videos).
- La creación o transmisión de material que cause cualquier tipo de molestia a los usuarios del HOSPITAL HUV.

- La circulación de información difamatoria de cualquier tipo, ya sea contra entidades o personas.
- Distribución de material que viole derechos de propiedad intelectual.
- Desarrollo de actividades que produzcan:
- La congestión de la red de comunicaciones o sistemas informáticos mediante el envío de información o programas concebidos para tal fin.
- La destrucción o modificación premeditada de la información de otros usuarios.
- La violación de la privacidad e intimidad de otros usuarios.
- El deterioro del trabajo de otros usuarios.
- Destrucción, manipulación o apropiación indebida de la información que circula por la red.
- Uso y obtención de cuentas de ordenador ajenas.
- Comunicación de contraseñas u otro tipo de información que permita a otros usuarios entrar en el sistema.
- Proporcionar accesos externos a la Red de datos del HOSPITAL HUV distintos de los que la Oficina Coordinadora de Gestión de la Información ofrece.
- La conexión de equipos de red activos (hubs, switches, routers, módems, firewalls, puntos de acceso inalámbricos, etc.) que previsiblemente perturbe el correcto funcionamiento de la misma o comprometa su seguridad, salvo expresa autorización de la Subgerencia Gestión de la Información.
- Conexión, desconexión o reubicación de equipos sin la autorización expresa de la Subgerencia Gestión de la Información.
- El alojamiento de dominios distintos de Hospital HUV es salvo expresa autorización de la Subgerencia Gestión de la Información.

Responsabilidades: Cuando se demuestre un uso incorrecto o no aceptable con respecto a lo especificado en este documento, la Oficina Coordinadora de Gestión de la Información procederá a la interrupción del servicio en el computador o dispositivo de red, dependiendo de la gravedad y reiteración del incidente.
Suspensión temporal o de emergencia del servicio: Esta medida se tomará cuando se produzca la violación de los términos de este documento de forma premeditada o cuando se esté causando una degradación en los recursos de la red y/o implique al HOSPITAL HUV en algún tipo de responsabilidad.
La acción consistirá en la desconexión física de la red de datos del HOSPITAL HUV, del computador o dispositivo móvil causante del incidente, hasta resolver la causa que ha llevado a tomar esta medida.
Donde no fuera posible la desconexión física se procederá al filtrado del tráfico del computador o dispositivo implicado.
Suspensión indefinida del servicio: Esta medida se aplicará cuando se incurra en infracciones de especial gravedad o en una reiterada violación de las condiciones de este documento, después de los correspondientes avisos por parte del personal de la Subgerencia Gestión de la Información. El servicio podrá restablecerse cuando se considere que las medidas adoptadas por el responsable del computador o dispositivo causante del incidente garantizan un uso aceptable en el futuro.
Cualquier usuario del HOSPITAL HUV que incumpla alguno de los términos especificados en este documento deberá asumir las responsabilidades derivadas de la utilización incorrecta de la infraestructura de la Red de datos del HOSPITAL HUV.
Cuando a un usuario de la Red de datos del HOSPITAL HUV se le haya aplicado alguna de las limitaciones en el servicio, podrá recurrir la suspensión ante la Subgerencia Gestión de la Información

6. ACCIONES DE CONTINGENCIA

Aplicable al Plan de Contingencia Sistemas de Informacion Misional (MOP-GDI-SIS-001)

7. ANEXOS

N/A

8. DOCUMENTOS RELACIONADOS

N/A

9. BIBLIOGRAFIA

- G.ES.06 Guia para la constuccion del PETI - Planeacion de la Tecnologia para la Transformacion

Digital. (MInTIC, Julio de 2019).
- Lienzo para la construcción del PETI.pptx
- Herramienta para la construcción del PETI.xlsx
- La Guía interactiva de implementación de la NTC 5854 (MinTIC, s.f.)
- Decreto Único Reglamentario del sector TIC 1008 de 2018 (cuyas disposiciones se compilan en el Decreto 1078 de 2015)
- Marco de Referencia de Arquitectura Empresarial (MInTIC, 2018)
- Marco de interoperabilidad (MinTIC, s.f.)
- Leguaje Común de Intercambio de Información (MinTIC, s.f.)
- Documentos y manuales (MinTIC, s.f.)
- La Guía interactiva de implementación de la NTC 5854 (MinTIC, s.f.)

Elaboró:	Revisó:	Aprobó:
Equipo de Gestión de la Información Profesional Administrativo Gestión de la Información		

Alberto Sánchez @ 2020-01-31, 16:36:24