	HOSPITAL UNIVERSITARIO DEL VALLE "EVARISTO GARCIA" E.S.E	**CÓDIGO:**	POL-HUV-HUV-003
		VERSIÓN:	003
	POLÍTICA DE SEGURIDAD DIGITAL	**FECHA DE EMISIÓN:**	2021-04-13

1. 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.

ESPECIFICOS:

Establecer y mantener la política de Seguridad Digital.
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 la política de seguridad Digital, en todos los niveles del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE.
Establecer las bases fundamentales para la protección de los activos de la información ya sean físicos o electrónicos.

2. ALCANCE

Este documento presenta los aspectos claves para la implementación de la Política de Seguridad Digital en el HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE conforme a lo estipulado en la norma NTC –ISO/IEC 27001. Es así como se define un alcance para la política, la organización para un modelo de gestión y los aspectos para el establecimiento, implementación, operación y seguimiento.
Este documento va dirigido e involucra a todo el personal del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE y a todos los niveles de la organización, debido a que la implementación, operación y cumplimiento de lo dispuesto en la Política de Seguridad Digital - PSD es responsabilidad de todo el talento humano como parte de las actividades diarias.

3. RESPONSABILIDAD

- Jefe de Oficina Coordinadora Gestion de la Informacion: Revisar y ajustar el documento.
- Oficina Juridica: Revisar y ajustar el documento a las normas y lineamientos de la institucion.
- Profesional de Sistemas Infraestructura: Socialización e implementación del documento.

4. 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 políticas, 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, las 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.

PSD: Política de Seguridad Digital

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.

5. POLÍTICA

La política en Informática son el conjunto de ordenamientos y lineamientos enmarcados en el ámbito jurídico y administrativo del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” 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.
El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” E.S.E. deberá contar con un Jefe o responsable del Área de Gestión de la información, 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 Oficina Coordinadora 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 Oficina Coordinadora de Gestion de la Información.

- Integración de sistemas y bases de datos del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” 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.

Las normas por las que se rige el PSD se encuentran contempladas en el marco Legal que hace parte de cada uno de los procedimientos que integran el documento:

- 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.
- 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 -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.

- Ley 1712 TRANSPARENCIA Y ACCESO A LA INFORMACIÓN PÚBLICA.

La política de Seguridad Digital pretende instituir y afianzar la cultura de seguridad de la información entre los funcionarios, personal externo y proveedores del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE. Por tal razón, es necesario que las violaciones a la política Seguridad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos y mitigar posibles afectaciones contra la seguridad de la información. Las medidas correctivas pueden considerar desde acciones administrativas, hasta acciones de orden disciplinario o penal, de acuerdo con las circunstancias, si así lo ameritan. Se consideran violaciones graves el robo, daño, divulgación de información reservada o confidencial de las dependencias del HUV, o de que se le declare culpable de un delito informático.

6. DESARROLLO DE LA POLÍTICA

La Oficina Coordinadora de Gestión de la Información establece la administración de la seguridad de los sistemas de información para toda la comunidad del Hospital Universitario del Valle “Evaristo García” ESE, a través de las siguientes lienamientos:

LINEAMIENTO DE SEGURIDAD DIGITAL

La Política de Seguridad Digital PSD es parte del sistema integrado de gestión del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, basado en un enfoque de gestión de riesgos de seguridad de la información de los procesos, en el contexto de los riesgos globales de la Institución, para: establecer, implementar, operar, hacer seguimiento, mantener y mejorar la seguridad de la información.

La seguridad de la información es una gestión continua para preservar las propiedades de confidencialidad, integridad y disponibilidad en los sistemas de información que manejan los procesos de la institución, basados en su nivel de riesgo.

La PSD permite a la institución identificar, implementar, mantener y mejorar los controles que requiere para tratar los riesgos de seguridad de la información, y llevarlos a niveles aceptables, de tal forma que estos controles sean los mínimos suficientes para proporcionar un ambiente de control y seguridad adecuados.

Los lineamientos de la Política de seguridad Digital son aplicables a cualquier proceso de la HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, sin importar su tamaño o función, dado que la implementación de la política debe ser proporcional a la criticidad de los activos de información que maneja y los riesgos identificados en los mismos.

La Política se estructura en el modelo gerencial Planificar – Hacer – Verificar - Actuar (PHVA) de tal forma que se pueda abordar la Planificación del sistema a través del establecimiento del Sistema PSD, el Hacer a través de su implementación y operación, la Verificación a través del seguimiento y revisión y el Actuar por medio del mantenimiento y mejora del Sistema PSD.

El Sistema PSD se integrará con otros sistemas de gestión tanto en distintas actividades como en diferentes etapas del ciclo PHVA, los cuales han sido definidos previamente, en el Plan Estratégico de la Alta Gerencia.

ESTRUCTURA BASADO EN PROCESOS:

El Sistema PSD 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 Sistema de Seguridad de Gestión 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 HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE 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 HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE 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 PSD.
- Hacer y mantener un seguimiento y una revisión permanente al desempeño y a la eficacia del Sistema PSD.
- La mejora continúa basada en la medición de los objetivos planteados inicialmente.

Basado en el énfasis planteado, el Sistema 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 Sistema PSD.

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 PSD y la revisión por la alta Gerencia, para lograr la mejora continua del sistema.

LINEAMIENTOS DE SEGURIDAD DEL PERSONAL

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, reconoce la importancia que tiene el factor talento humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos funcionarios se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los funcionarios en sus cargos.

Todo el personal nuevo en la institución deberá recibir la inducción sobre la política de seguridad digital, donde se den a conocer las obligaciones y deberes para los usuarios y las sanciones en que pueden incurrir en caso de incumplimiento.

- Es responsabilidad del usuario o funcionario evitar en todo momento la fuga de información de la entidad que se encuentre almacenada en los equipos de cómputo que tengan asignados.
- Será responsabilidad del usuario solicitar la capacitación necesaria para el manejo de las herramientas de la información que se utilizan en su equipo, a fin de evitar riesgos por mal uso y para aprovechar al máximo las mismas.
- Creación de Usuarios: Toda persona que ingresa como usuario nuevo al Hospital Universitario del Valle “Evaristo García” ESE, debe aceptar las condiciones de confidencialidad, de uso adecuado de los bienes informáticos y de la información, así como cumplir y respetar al pie de la letra las directrices impartidas en laspolítica de Seguridad de Gestión de la información (PSD).
- Creación de Usuarios Clínicos: Todo el personal clínico nuevo que ingrese a la Institución, deberá acercarse a la Oficina Coordinadora de Gestión de la Información con el “Formato Creación de Usuarios Historia Clínica Electrónica”, debidamente diligenciado y con las firmas que avalan su vinculación.
- Creación de Usuarios Administrativos: Todo el personal administrativo nuevo que ingrese a la Institución, deberá acercarse a la Oficina Coordinadora de Gestión de la Información con el “Formato Creación Usuarios Administrativos”, debidamente diligenciado y con las firmas que avalan su vinculación.
- Inactivación de Usuarios: Toda persona que se desvincule de la institución debe ser notificada al área de gestión de la información para realizar la desactivación del login a los sistemas de información que se administran en esta área.
- Los desarrolladores deben asegurar que los sistemas de información construidos requieran autenticación para todos los recursos y páginas, excepto aquellas específicamente clasificadas como públicas.
- Los desarrolladores deben certificar la confiabilidad de los controles de autenticación, utilizando implementaciones centralizadas para dichos controles.
- Los desarrolladores deben certificar que no se almacenen contraseñas, cadenas de conexión u otra información sensible en texto claro y que se implementen controles de integridad de dichas contraseñas.
- Los desarrolladores deben establecer los controles de autenticación de tal manera que cuando fallen, lo hagan de una forma segura, evitando indicar específicamente cual fue la falla durante el proceso de autenticación y, en su lugar, generando mensajes generales de falla.
- Los desarrolladores deben asegurar que no se despliegan en la pantalla las contraseñas ingresadas, así como deben deshabilitar la funcionalidad de recordar campos de contraseñas.

GESTION DE ACTIVOS DE INFORMACION

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) propiedad del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, son activos de la institución y se proporcionan a los funcionarios y terceros autorizados, para cumplir con los propósitos del negocio.

Toda la información sensible del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que dicte la Oficina de Activos de Inventarios y la Oficina Coordinadora de Gestion de la Información. Los propietarios de los activos de información deben llevar a cabo el levantamiento y la actualización permanente del inventario de activos de información al interior de sus procesos o áreas.

- Los usuarios no deben mover o reubicar los equipos de cómputo, instalar o desinstalar dispositivos, ni retirar sellos de los mismos sin la autorización de la Oficina Coordinadora de Gestion de la Información, en caso de requerir este servicio deberá solicitarlo.
- El Área de Inventarios de activos será la encargada de generar el resguardo y recabar la firma del usuario informático como responsable de los activos informáticos que se le asignen y de conservarlos en la ubicación autorizada por la Oficina Coordinadora de Gestion de la Información.
- El equipo de cómputo asignado, deberá ser para uso exclusivo de las labores de los funcionarios o servidores públicos del Hospital Universitario del Valle “Evaristo García”.
- Mientras se opera el equipo de cómputo, no se deberán consumir alimentos o ingerir líquidos.
- Se debe evitar colocar objetos encima del equipo cómputo o tapar las salidas de ventilación del monitor o de la CPU.
- Se debe mantener el equipo informático en un lugar limpio y sin humedad.
- El usuario debe asegurarse que los cables de conexión no sean pisados al colocar otros objetos cerca o contra ellos, en caso de que no se cumpla, solicitar su reubicación y la organización de cables de red con el personal de la Oficina Coordinadora de Gestion de la Información, o el cableado eléctrico con la Subgerencia Técnica.
- Cuando se requiera realizar cambios múltiples de los equipo de cómputo derivado de reubicación de lugares físicos de trabajo o cambios locativos, éstos deberán ser notificados con cinco días de anticipación a la Oficina Coordinadora de Gestion de la Información a través de un plan detallado y al área de Inventarios.
- Por ningún motivo el usuario o funcionario distinto al personal de la Oficina Coordinadora de Gestion de la Información abra o destape los equipos de cómputo.

- Todas las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos son asignados a un responsable, por lo cual es su compromiso hacer uso adecuado y eficiente de dichos recursos.

- En el momento de desvinculación o cambio de labores, los funcionarios deben realizar la entrega de su puesto de trabajo al Director o Jefe de Área y/o Servicio o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

- El servidor o funcionario que tengan bajo su responsabilidad o asignados algún equipo de cómputo, será responsable de su uso y custodia; en consecuencia, responderá por dicho bien de acuerdo a la normatividad vigente en los casos de robo, extravío o pérdida del mismo.

- El servidor o funcionario deberán dar aviso inmediato a la Oficina Coordinadora de Gestion de la Información, a la Oficina de Seguridad y al Área de Inventarios de Activos de la desaparición, robo o extravío de equipos de cómputo, periféricos o accesorios bajo su responsabilidad.

- Los propietarios de los activos de información deben autorizar los accesos a sus sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, acogiendo los procedimientos establecidos.

- Los propietarios de los activos de información deben monitorear periódicamente los perfiles definidos en los sistemas de información y los privilegios asignados a los usuarios que acceden a ellos.

- La Oficina Coordinadora de Gestión de la Información debe establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

- La Oficina Coordinadora de Gestión de la Información debe asegurar, mediante los controles necesarios, que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción, y así mismo que los menús muestren los mensajes de identificación apropiados para reducir los riesgos de error.

- La Oficina Coordinadora de Gestión de la Información debe establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información; así mismo, debe asegurarse que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

- La Oficina Coordinadora de Gestión de la Información debe proporcionar repositorios de archivos fuente de los sistemas de información; estos deben contar con acceso controlado y restricción de privilegios, además de un registro de acceso a dichos archivos.

LINEAMIENTO DE MANEJO DE INFORMACION

- Con base en este documento el Proceso de comunicaciones y Gestión de la Información define acciones para el mejoramiento de los sistemas de información actualmente en producción, garantiza el cumplimiento en la normatividad vigente y el suministro de información a entes de control externo e interno así como a las subdirecciones de servicios. De igual manera este documento le permite conocer y evaluar las soluciones informáticas que requiere el Hospital para mejorar su integralidad, calidad, oportunidad, eficiencia y eficacia que se deben construir a partir del registro de información en sistemas basados en la Historia clínica Electrónica.
- De igual manera la institución cuenta con herramientas que permiten identificar continuamente necesidades de información, recursos, productividad y direccionamiento de forma sistemática y organizada:

    - Planes de Inversión, Presupuestos y Planes Operativos.
    - Plan de Desarrollo Institucional
    - Plan de Capacitación Institucional.
    - Manuales de Procedimiento, guías y protocolos de cada una de las unidades.
    - Encuestas de Satisfacción, Documentos del Comité Docente – Asistencial CODA, del Hospital HUV del Valle,política de Calidad,política de Comunicaciones,política de Seguridad del Paciente.
    - Documentos derivados de la implementación del Sistema de Gestión Integral de la Calidad del Hospital Universitario del Valle “Evaristo García” E.S.E.

- Análisis de la Información: Cada unidad operativa de la institución establece sus necesidades particulares de información las cuales solicita mediante requerimientos, los cuales deben ser lo más claros y coherentes posibles para que esta unidad pueda ejecutar la tarea lo mejor posible y se encarga de diseñar, producir y socializar la solución con lo cual se garantiza autonomía y responsabilidad a las unidades operativas en la valoración de su información.
- Transmisión de la Información: El esquema de divulgación de la información analizada por cada una de las unidades operativas es solo pertinencia de los subgerentes y/o gerentes de cada área, dado que la Oficina Coordinadora de Gestion de la Información solo es un apoyo en la instalación, configuración de software de herramientas colaborativas, garantiza la disponibilidad de los elementos para el funcionamiento de los sistemas de información de misión crítica y las conexiones internas o externas a redes de datos.
- Implementación de Herramientas: Como quiera que la Oficina Coordinadora de Gestion de la Información es un componente que brinda apoyo tecnológico a la institución, participa de forma activa en las actividades de instalación, configuración y parametrización de las diferentes herramientas informáticas establecidas como proyectos de acuerdo con el plan de desarrollo institucional o acordado en los planes de desarrollo anuales.
-
- De cualquier manera la dinámica de la institución requiere de incorporar nuevas tecnologías informáticas en ocasiones no contempladas en el plan de desarrollo, pero que demanda de la inminente aplicación de las mismas.
- Para estas actividades la Oficina Coordinadora de Gestion de la Información siguiendo los lineamientos de apoyo de sistemas y el comité directivo hace ajustes o proyectos

encaminados en ofrecer entornos adecuados para la automatización de procesos de acuerdo con las prioridades que establece la dinámica de la institución, siguiendo metodologías y esquemas adecuados de acuerdo con los parámetros emanado por la Ingeniería de Software.

- La implementación de herramientas no está basado exclusivamente en la actividad de instalación, configuración y parametrización, sino que requiere el concurso directo de los líderes de los procesos y la adecuada interiorización y aplicación de las herramientas por parte de los usuarios finales.
- Se entiende que los líderes de procesos nombran de su equipo de trabajo a personas idóneas y con la experticia necesaria para definirlos como líderes funcionales de las soluciones que se implementen como apoyo a su área. La Oficina Coordinadora de Gestion de la Información nombrará en el caso de ser necesario, el líder técnico para el acompañamiento que sea requerido.
- Almacenamiento, Conservación y Depuración de la Información: La Oficina Coordinadora de Gestion de la Información no es responsable de los principios y normatividad relacionados con estos ítems, solo establece y garantiza todo lo relacionado con la información de sistemas misionales y de misión crítica de almacenamiento, conservación y depuración de la información base (sistemas operativos, Sistemas de gestión de bases de datos, logs de transacciones, etc.).
- Lo relacionado con la información específica de cada UES u Áreas Administrativa, Financiera o Misional, es de responsabilidad directa del usuario. La Oficina Coordinadora de Gestion de la Información garantizará la operación de un File Server para que el usuario cuente con una herramienta adicional para conservación de la información a las unidades operativas que así lo requieran.
- La custodia de este File Server estará bajo la responsabilidad del equipo de infraestructura de la Oficina Coordinadora de Gestion de la Información, pero la gestión de uso del mismo estará a cargo de cada unidad.
- Seguridad y Confidencialidad de la Información: Como todo componente fundamental en los sistemas de Información del HUV, el acceso a los datos es responsabilidad de los mecanismos y perfiles de usuario que validen en cada módulo, teniendo como base:
-
  - Debe existir solicitud por escrito de los sistemas que el usuario requiere acceder.
  - Se creara un solo login (usuario) para los diferentes sistemas que el usuario requiera y desde allí se validara según el perfil las opciones que tiene permitidas.
  - El login deberá ser exclusivamente de uso personal, por ningún motivo puede ser trasferible con otros usuarios para acceder al sistema.
  - Dependiendo del grupo y/o perfil de usuario el sistema permitirá las operaciones que el usuario tiene asignadas.
  - Para futuros sistemas de información (HCL, HIS, RIS, LIS, OIS) la información sensible como diagnósticos – procedimientos que son de pertinencia del paciente y su médico deberán ser solo visualizados por el personal autorizado y no de conocimiento público.
  - Aunque se tenga acceso a la información, se incurre en un delito al consultar o manipular información sin la debida autorización.

- Entrega de Información: La entrega de información solicitada por la Oficina Coordinadora de Gestion de la Información para los procesos de implementación, ajuste y/o mejora a los módulos de sistemas de información de misión crítica, deben tener la certificación del líder funcional del área.
- En ningún caso se debe delegar por parte del líder funcional o del proceso la consecución, validación y depuración de información al equipo técnico de sistemas.
- Toda información que la Oficina Coordinadora de Gestion de la Información procese y sea entregada por diferentes medios físicos y/o magnéticos, será soportado con un documento

de requerimiento, donde se establezcan los parámetros de ejecución, el solicitante y la confirmación de la recepción de la misma.

- Para el caso la información solicitada por los entes de control (fiscalía, Contraloría, etc.) se debe tener la certificación de solicitud por la ventanilla única, aprobación del correspondiente líder de proceso (de acuerdo con lo establecido en laspolítica de Confidencialidad), para garantizar tiempos y responsables de la información solicitada.
- En el caso de información requerida se relacione con datos sensible o de confidencialidad al paciente y/o a la institución se debe velar por la responsabilidad y seguridad en el manejo, control y uso que se le dará a la información entregada, tal como lo defina la política de confidencialidad.
- Para cualquier caso la información solo podrá ser solicitada por el proceso administrador de la misma, mediante solicitud del Líder, Jefe o subgerente del área y/o servicio. Así mismo la entrega después de su procesamiento, se hará al responsable solicitante quien la debe hacer llegar a los entes externos en caso de requerirse.
- Bajo ninguna circunstancia la Oficina Coordinadora de Gestion de la Información procesará información solicitada directamente por entes externos, para lo cual se remitirá a la oficina jurídica, de control o Gerencia correspondiente para su aprobación.
- Respaldo de Información: Los datos de los sistemas de información, deben ser respaldados de acuerdo a la frecuencia de actualización de sus datos, rotando los dispositivos de respaldo y guardando respaldos históricos periódicamente. Es indispensable llevar una bitácora oficial de los respaldos realizados, así mismo, las cintas, discos o dispositivos de respaldo deberán guardarse en un lugar de acceso restringido con condiciones ambientales suficientes para garantizar su conservación.
- En caso de información vital para el funcionamiento del área, se deberán tener procesos definidos, así como tener el respaldo diario de las modificaciones efectuadas, rotando los dispositivos de respaldo y guardando respaldos periódicamente, para el caso de la información centralizada del H.U.V.
- En cuanto a la información de los equipos de cómputo personales, la Subgerencia de Gestión de la Información recomienda a los usuarios que realicen sus propios respaldos en la red o en medios de almacenamientos alternos y con una periodicidad no mayor a ocho (8) días.
- La información necesaria pero no indispensable, deberá ser respaldada con una frecuencia mínima de una semana, rotando los dispositivos de respaldo y guardando respaldos históricos mensualmente.
- El respaldo de la información ocasional o eventual queda a criterio del área.
- Es obligación del funcionario encargado de las copias de respaldo, la entrega conveniente de los archivos magnéticos de información, a quien le suceda en el cargo.
- Generación de Informes: Todo informe que se requiera obtener a través del sistema central de datos, debe ser solicitado por el Subgerente de unidad o por el Jefe de área, justificando el uso del mismo.
- Mensaje enviado por oficio escrito o por correo electrónico.
- Debe especificar el tipo de informe, las variables y los períodos de trabajo, ser lo más explícito posible.
- Si el informe es requerido por un ente externo, toda solicitud debe estar oficiada por medio físico en papelería con membrete de la institución solicitante.
- Oficio Dirigido a la Gerencia General del H.U.V., u oficina responsable.La Gerencia o la jefatura del área evaluará la viabilidad o delegará a algún subgerente el impacto de entrega de los datos a un ente externo.Solo si la Gerencia General o la Jefatura del área lo solicita, se entregará información en medio magnético, toda vez que esto es susceptible a manipulación por parte de terceros.El oficio con la firma de aprobación de la Gerencia

General o Jefatura del Área se entregará a la Oficina Coordinadora de Gestion de la Información para proceder a asignarlo al analista correspondiente.
- Los datos correspondientes a información de medios magnéticos de acuerdo con parámetros preestablecidos, leyes u otros que sean de carácter gubernamental el Subdirector responsable se soportará con el texto de la correspondiente ley.
- Por ningún motivo la Oficina Coordinadora de Gestion de la Información o miembro alguno, está autorizado a generar información a terceros ni a entregarla, aun cuando se presenten funcionarios con identificación alguna a solicitar los datos.

LINEAMIENTOS DE CONTROL DE ACCESO

La Oficina Coordinadora de Gestion de la Información del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, como responsable de las redes de datos y los recursos de red de la institución, debe propender porque dichas redes sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico.

- Para el acceso a los sitios y áreas restringidas como cuartos de cableado, se debe notificar a la Oficina Coordinadora de Gestion de la Información para la autorización correspondiente, y así proteger la información y los bienes informáticos. Por esta razón se manejan chapas de seguridad en cada uno de los cuartos de cableados y estas llaves solo las maneja esta subgerencia.
- El usuario o funcionario deberán reportar de forma inmediata a la Oficina Coordinadora de Gestion de la Información cuando se detecte riesgo alguno real o potencial sobre equipos de cómputo o de comunicaciones, tales como caídas de agua, choques eléctricos, caídas o golpes o peligro de incendio.
- Cualquier persona que tenga acceso a las instalaciones de Hospital Universitario del Valle “Evaristo García”, deberá registrar al momento de su entrada, el equipo de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad de la entidad, en el área de recepción o portería, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de salida correspondiente, en la Oficina de Seguridad.
- Las computadoras personales, las computadoras portátiles, y cualquier activo de tecnología de información, podrá ser retirado de las instalaciones de Hospital Universitario del Valle “Evaristo García” ESE, únicamente con la autorización de salida de la Oficina de Seguridad, anexando el comunicado de autorización del equipo debidamente firmado por el Jefe del área, Jefe de Seguridad o por el Jefe de la Oficina Coordinadora de Gestion de la Información.
- El control de acceso a todos los Sistemas de Información de la entidad debe realizarse por medio de códigos de identificación y palabras claves o contraseñas únicos para cada usuario.
- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de información del HUV debe ser asignado de acuerdo a la identificación previa de requerimientos de seguridad y de la Institución, que se definan por las diferentes dependencias del Hospital HUV, así como normas legales o leyes aplicables a la protección de acceso a la información presente en los sistemas de información.
- Los responsables de la administración de la infraestructura tecnológica del Hospital HUV asignan los accesos a plataformas, usuarios y segmentos de red de acuerdo a los protocolos y procedimientos establecidos.
- Todos y cada uno de los equipos de cómputo son asignados a un responsable, por lo que es de su competencia hacer buen uso de los mismos.
- La Oficina Coordinadora de Gestion de la Información es responsable de proporcionar a los usuarios el acceso a los recursos informáticos.

- El acceso lógico a equipo especializado de cómputo (servidores, enrutadores, bases de datos, etc.) conectado a la red del HUV es administrado por la Oficina Coordinadora de Gestion de la Información.
- La Oficina Coordinadora de Gestion de la Información debe asegurar que las redes inalámbricas del Hospital HUV cuenten con métodos de autenticación que evite accesos no autorizados.
- La Oficina Coordinadora de Gestion de la Información, en conjunto con la Subgerencia Técnica y la Oficina de Seguridad, deben establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, así como velar por la aceptación de las responsabilidades de dicho terceros. Además, se debe formalizar la aceptación de laspolítica de Seguridad de la Información por parte de estos.
- Los funcionarios y personal provisto por terceras partes, antes de contar con acceso lógico por primera vez a la red de datos del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, deben contar con el formato de creación de cuentas de usuario debidamente autorizado y el Acuerdo de Confidencialidad firmado previamente.
- Los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos del hospital HUV deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

LINEAMIENTOS DE ACCESO REMOTO

La presente política contempla las comunicaciones electrónicas y conexiones remotas de usuarios autorizados para acceder a los servicios de la red de datos institucional.

- El Servicio de acceso remoto permite el ingreso a la red de datos institucional a aquellos usuarios externos e internos expresamente autorizados por la Oficina Coordinadora de Gestion de la Información, para que lo hagan desde redes externas o internas, el cual debe estar sujeto a autenticación con un nivel adecuado de protección.
- Solo Los equipos de procesamiento de datos tipo servidor y de comunicación tendrán habilitado el servicio de conexión de acceso remoto. Los clientes para acceder a estos recursos serán previamente identificados y autorizados.
- La Oficina Coordinadora de Gestion de la Información debe implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE.
- La Oficina Coordinadora de Gestion de la Información debe restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las labores desempeñadas.
- La Oficina Coordinadora de Gestion de la Información debe verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE de manera permanente.
- Los usuarios que realizan conexión remota deben contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE y deben acatar las condiciones de uso establecidas para dichas conexiones.
- Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores públicos, de hoteles o salas internet, entre otros.

LINEAMIENTOS DE ENCRIPTACION Y CRIPTOGRAFIA

La Oficina Coordinadora de Gestion de la Información velará porque la información del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

- La Oficina Coordinadora de Gestion de la Información debe almacenar y/o transmitir la información digital clasificada como reservada o restringida bajo técnicas de cifrado con el propósito de proteger su confidencialidad e integridad.
- La Oficina Coordinadora de Gestion de la Información debe verificar que todo sistema de información o aplicativo que requiera realizar transmisión de información reservada o restringida, cuente con mecanismos de cifrado de datos.
- La Oficina Coordinadora de Gestion de la Información debe desarrollar y establecer estándares, procedimientos para el manejo, administración de llaves de cifrado y la aplicación de controles criptográficos.
- Los desarrolladores deben cifrar la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.
- Se recomienda utilizar el Software WinPT de licencia GNU, para el cifrado y generación de llaves, las cuales tendrán fecha de inicio y caducidad de vigencia.
- Los desarrolladores deben asegurarse que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la Oficina Coordinadora de Gestion de la Información.
- Se desarrollarán lineamientos respecto de la administración de claves, de la recuperación de información cifrada en caso de pérdida, compromiso o daño de las claves y en cuanto al reemplazo de las claves de cifrado.
- Para el resguardo de información, cuando así surja de la evaluación de riesgos realizada por el propietario de la información y el responsable de seguridad informática.
- Las llaves criptográficas utilizadas para el cifrado de los datos deben estar clasificadas como confidencial y ser protegidas contra divulgación, uso indebido o sustitución no autorizada restringiendo al mínimo el número de custodios necesarios y guardándola de forma segura en la menor cantidad de ubicaciones y formas posibles.

LINEAMIENTOS DE SEGURIDAD FISICA Y MEDIO AMBIENTE

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus áreas. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

- Las solicitudes de acceso al centro de cómputo o a los centros de cableado deben ser aprobadas por funcionarios de la Oficina Coordinadora de Gestion de la Información autorizados; no obstante, los visitantes siempre deberán estar acompañados de un funcionario de dicha oficina durante su visita al centro de cómputo o los centros de cableado.
- La Oficina Coordinadora de Gestion de la Información debe registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.
- La Oficina Coordinadora de Gestion de la Información debe descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de

cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las labores de un funcionario autorizado.

- La Oficina Coordinadora de Gestion de la Información debe proveer las condiciones físicas y medioambientales necesarias para certificar la protección y correcta operación de los recursos de la plataforma tecnológica ubicados en el centro de cómputo; deben existir sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de descarga eléctrica, sistemas de vigilancia y monitoreo y alarmas en caso de detectarse condiciones ambientales inapropiadas. Estos sistemas se deben monitorear de manera permanente.
- La Oficina Coordinadora de Gestion de la Información debe velar porque los recursos de la plataforma tecnológica del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE ubicados en el centro de cómputo se encuentran protegidos contra fallas o interrupciones eléctricas.
- La Oficina Coordinadora de Gestion de la Información debe certificar que el centro de cómputo y los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.
- La Oficina Coordinadora de Gestion de la Información debe asegurar que las labores de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.
- La conservación en condiciones seguras de estos documentos se efectúa en locales especialmente habilitados, al amparo de desastres naturales o accidentales, de robos o usos indebidos, de campos magnéticos o de diferencias térmicas o hidrométricas excesivas.
- Los equipos para uso interno se instalarán en lugares adecuados, lejos de polvo y riesgo de daño. En las áreas de atención directa al público los equipos se instalarán en lugares adecuados.
- La Oficina Coordinadora de Gestion de la Información, así como las áreas operativas deberán contar con un croquis actualizado de las instalaciones de comunicaciones de los equipos de cómputo en red.
- Las instalaciones eléctricas y de comunicaciones, estarán de preferencia fija o en su defecto resguardadas del paso de personas o máquinas, y libres de cualquier interferencia eléctrica o magnética.
- Las instalaciones se apegarán estrictamente a los requerimientos de los equipos, cuidando las especificaciones del cableado y de los circuitos de protección necesarios.
- En ningún caso se permitirán instalaciones improvisadas o sobrecargadas.
- Cuando en la instalación se alimenten elevadores, motores y maquinaria pesada, se deberá tener un circuito independiente, exclusivo para el equipo y/o red de cómputo.
- Para el caso de los sistemas de conectividad de datos se evitará, salvo circunstancias extremas, el uso de “cascadas” de red.
- La instalación de equipos de cómputo, dispositivos de conectividad o cualquier otro elemento de informática o telemática de un ente externo al Hospital HUV debe tener la autorización de la Gerencia General y la Oficina Asesora de Planeación, toda vez que deben de definir la distribución de la obra civil y la no afectación de nuevos proyectos del HUV.
- Planeación debe evaluar el impacto sobre nuevas obras u obras en proceso.
- La Oficina Coordinadora de Gestion de la Información aportará la información correspondiente a centros de cableado o distribución adecuada para llevar a cabo los proyectos.
- Es obligación de la Oficina Coordinadora de Gestion de la Información vigilar que el equipo de cómputo se use bajo las condiciones especificadas por el proveedor y de acuerdo a las funciones del área a la que se asigne.
- La seguridad física de los dispositivos informáticos, así como el adecuado uso y operación, manipulación de piezas y componentes, estará bajo la responsabilidad del Jefe del Área donde se instalen los equipos.

- Los colaboradores de la empresa al usar los equipos de cómputo, se abstendrán de consumir alimentos, fumar o realizar actos que perjudiquen el funcionamiento de los mismos o deterioren la información almacenada en medios magnéticos, ópticos, etc.
- En caso de daño sobre algún dispositivo, propio o arrendado, la Oficina de Control Interno emitirá el procedimiento de responsabilidad, aún económica, sobre el bien.
- Mantener claves de acceso que permitan el uso solamente al personal autorizado para ello.
- Verificar la información que provenga de fuentes externas a fin de corroborar que estén libres de cualquier agente externo que pueda contaminarla o perjudique el funcionamiento de los equipos.
- Mantener pólizas de seguros de los recursos informáticos en funcionamiento.
- Con el fin de proteger perímetros en los cuales se encuentre información Institucional, la Oficina Coordinadora de Gestion de la Información instalará los elementos necesarios para restringir el acceso del personal no autorizado al hospital HUV.
- Como mecanismo de prevención todos los empleados y visitantes no deben comer, fumar o beber en el Data Center o en instalaciones donde haya equipos tecnológicos.
- No se debe proveer información sobre la ubicación del Data Center o de los lugares críticos, como mecanismo de seguridad.
- Cualquier persona que tenga acceso a las instalaciones del Hospital HUV deberá registrar al momento de su entrada en las porterías, el ingreso de equipos de cómputo, equipo de comunicaciones, medios de almacenamiento y herramientas que no sean propiedad del hospital, el cual podrán retirar el mismo día. En caso contrario deberá tramitar la autorización de la salida correspondiente.

LINEAMIENTOS DE SEGURIDAD OPERATIVA

La Oficina Coordinadora de Gestion de la Información, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, asignará funciones específicas a sus funcionarios, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades.

Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

La Oficina Coordinadora de Gestion de la Información proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información del hospital HUV, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

La Oficina Coordinadora de Gestion de la Información debe efectuar, a través de sus funcionarios, la documentación y actualización de los procedimientos relacionados con la operación y administración de la plataforma tecnológica del hospital HUV.

La Oficina Coordinadora de Gestion de la Información debe proporcionar a sus funcionarios manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE.

La Oficina Coordinadora de Gestion de la Información debe proveer los recursos necesarios para la implantación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores,

editores o fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

La Oficina Coordinadora de Gestion de la Información, a través de sus funcionarios, debe realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

Credenciales de Acceso: Los usuarios son los únicos responsables por la seguridad de sus credenciales de acceso (Usuario y Contraseña), las cuales son de uso exclusivo e intransferible.

Instalación, mantenimiento y actualización de hardware: El personal de Soporte Técnico es el único autorizado para instalar aplicaciones y realizar mantenimientos preventivos y correctivos en los equipos de cómputo del hospital HUV.

Uso de los Equipos de Cómputo: Los equipos de cómputo (computadores, impresoras, portátiles, servidores, tablas y demás elementos similares) de la Institución serán utilizados únicamente por el personal autorizado para el desarrollo de las actividades asignadas.

Todo funcionario, contratista y/o clínico de la Institución es responsable del equipo que le sea asignado; el cual será asignado a su inventario personal, de acuerdo con la oficina de Inventarios de activos.

Está prohibido retirar de las instalaciones del hospital cualquier equipo de cómputo. Si es necesario hacerlo, debe contar con la autorización de Servicios Generales en cabeza del Jefe de Seguridad y con el visto bueno del Jefe Inmediato. El personal de vigilancia deberá registrar la orden de salida de los equipos para su movilización fuera de las instalaciones del hospital HUV.

En caso de presentarse una falla o problema de hardware o software en una estación de trabajo o equipo portátil propiedad del hospital, el usuario responsable del mismo deberá informarlo a la Oficina Coordinadora de Gestion de la Información a través del HelpDesk o mesa de ayuda, para una asistencia especializada y, por ningún motivo, deberá intentar resolver el problema.

Se debe mantener el equipo de cómputo libre de fotos, calcomanías y cualquier otro elemento que lo pueda deteriorar o comprometer su integridad.

Para todos los equipos de cómputo propiedad de la Institución, se instalará únicamente el software que cuente con licencia autorizada para uso en el Hospital HUV. El software que no cumpla con estos lineamientos se debe desinstalar de manera inmediata para garantizar el cumplimiento de la Ley antipiratería. De igual manera en los computadores con sistema operativo Windows se instalará software antivirus que la Oficina Coordinadora de Gestion de la Información, establezca.

Los usuarios únicamente deben descargar archivos adjuntos que provengan de fuentes conocidas para evitar contaminación por virus informáticos y/o instalación de software malicioso en sus estaciones de trabajo o equipos portátiles.

Aplicaciones de Ofimática: La suite de ofimática permitida por la Institución para equipos con sistema operativo Windows y Mac, son las versiones de Microsoft Office licenciadas por la entidad. Además, se permite el uso de la versión libre de Open Office, en los equipos de cómputo propiedad del hospital.

La instalación de productos de software desarrollados por el grupo de Análisis de Sistemas de la Oficina Coordinadora de Gestion de la Información se realizará en los equipos de cómputo propiedad del hospital designados para tal fin.

Está prohibido manipular el código fuente de una aplicación sin la autorización correspondiente de la Oficina Coordinadora de Gestion de la Información, para generar cambios o mejoras a la misma. Si se requiere tener acceso al código fuente de una aplicación desarrollada en la institución, se debe solicitar permiso al jefe del área de sistemas. Si se trata de una aplicación desarrollada por un proveedor externo, se deben revisar las condiciones del contrato.

La Institución hospitalaria HUV se reserva el derecho de monitorear los equipos de cómputo, conectados a la red de datos del hospital, de los cuales se sospeche que están comprometiendo la confidencialidad, integridad y disponibilidad de la información.

Los usuarios solamente tendrán acceso a los servicios de red para cuyo uso están específicamente autorizados según su perfil.

El Hospital Universitario del Valle “Evaristo García” ESE dispone de un Data Center, como lugar adecuado para el alojamiento de los equipos de procesamiento de datos tipo servidor.

La Oficina Coordinadora de Gestion de la Información gestiona el mantenimiento periódico para el Data Center junto con los elementos que lo componen, para garantizar la integridad, disponibilidad y confidencialidad de los activos de información que se encuentran allí alojados.

Los usuarios no pueden portar información del hospital HUV clasificada como privada sin la previa autorización del propietario del activo de información independiente del medio que utilice.

La instalación de un nuevo componente en la red de datos debe estar autorizada por la Coordinación de Infraestructura de la Oficina Coordinadora de Gestion de la Información.

La adopción y uso de Tecnologías de la información y la comunicación orientadas a la gestión de servicios institucionales, serán aprobados por la Oficina Coordinadora de Gestion de la Información.

LINEAMIENTOS DE SEGURIDAD EN LAS COMUNICACIONES

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE establecerá, a través de la Oficina Coordinadora de Gestion de la Información, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida del hospital.

La Oficina Coordinadora de Gestion de la Información debe adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE.

La Oficina Coordinadora de Gestion de la Información debe implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

La Oficina Coordinadora de Gestion de la Información debe mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios, ubicación geográfica o cualquier otra tipificación que se considere conveniente para el Hospital HUV.

La Oficina Coordinadora de Gestion de la Información debe identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

La Oficina Coordinadora de Gestion de la Información debe establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica del Hospital HUV, acogiendo buenas prácticas de configuración segura.

La Oficina Coordinadora de Gestion de la Información, a través de sus funcionarios y la Coordinación de Infraestructura, debe identificar, justificar y documentar los servicios, protocolos y puertos permitidos por el hospital HUV en sus redes de datos.

La Oficina Coordinadora de Gestion de la Información debe instalar protección entre las redes internas del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE y cualquier red externa, que este fuera de la capacidad de control y administración del hospital HUV.

La Oficina Coordinadora de Gestion de la Información debe velar por la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE.

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre funcionarios y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

La Oficina Coordinadora de Gestion de la Información debe generar y divulgar un procedimiento para la administración de cuentas de correo electrónico.

La Oficina Coordinadora de Gestion de la Información debe diseñar y divulgar las directrices técnicas para el uso de los servicios de correo electrónico.

La Oficina Coordinadora de Gestion de la Información debe proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico.

La Oficina Coordinadora de Gestion de la Información debe establecer procedimientos e implantar controles que permitan detectar y proteger la plataforma de correo electrónico contra código malicioso que pudiera ser transmitido a través de los mensajes.

La Oficina Coordinadora de Gestion de la Información, con el apoyo de la Oficina de Educación y de la Oficina de Comunicaciones, deben generar campañas para concientizar tanto a los funcionarios internos, como al personal provisto por terceras partes, respecto a las precauciones que deben adoptar en el intercambio de información sensible por medio del correo electrónico.

La cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario del hospital o provisto por un tercero, bajo ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.

Los mensajes y la información contenida en los correos electrónicos deben ser relacionados con el desarrollo de las labores y funciones de cada usuario en apoyo al objetivo misional del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE. El correo institucional no debe ser utilizado para actividades personales.

Los mensajes y la información contenida en los buzones de correo son propiedad del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

Los usuarios de correo electrónico institucional tienen prohibido él envió de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana y resulten ofensivas para los funcionarios del hospital HUV y el personal provisto por terceras partes.

No es permitido el envío de archivos que contengan extensiones ejecutables, bajo ninguna circunstancia.

Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por el HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en el Hospital HUV.

La Oficina Coordinadora de Gestion de la Información debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

La Oficina Coordinadora de Gestion de la Información debe diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

La Oficina Coordinadora de Gestion de la Información debe monitorear continuamente el canal o canales del servicio de Internet.

La Oficina Coordinadora de Gestion de la Información debe establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

La Oficina Coordinadora de Gestion de la Información debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Los usuarios del servicio de Internet del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE deben hacer uso del mismo en relación con las actividades laborales que así lo requieran.

Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores.

No está permitido el acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes opolítica establecidas en este documento.

Los usuarios del servicio de internet tienen prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Facebook, Kazaa, MSN, Yahoo, Sype, Net2phome y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines

diferentes a las actividades propias del negocio del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE.

No está permitido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Oficina Coordinadora de Gestion de la Información, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

No está permitido el intercambio no autorizado de información de propiedad del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, de sus clientes y/o de sus funcionarios, con terceros.

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE asegurará la protección de la información en el momento de ser transferida o intercambiada con otras entidades y establecerá los procedimientos y controles necesarios para el intercambio de información; así mismo, se establecerán Acuerdos de Confidencialidad y/o de Intercambio de Información con las terceras partes con quienes se realice dicho intercambio. El hospital HUV propenderá por el uso de tecnologías informáticas y de telecomunicaciones para llevar a cabo el intercambio de información; sin embargo, establecerá directrices para el intercambio de información en medio físico.

LINEAMIENTOS DE DESARROLLO SISTEMAS DE INFORMACION

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE asegurará que el software adquirido y desarrollado tanto al interior de la institución, como por terceras partes, cumplirá con los requisitos de seguridad y calidad establecidos por él. Las áreas propietarias de sistemas de información, la Oficina Coordinadora de Gestion de la Información incluirán requisitos de seguridad en la definición de requerimientos y, posteriormente se asegurarán que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido.

Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro del hospital HUV formalmente asignada.

La Oficina Coordinadora de Gestion de la Información debe establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro, con el fin de proporcionar a los desarrolladores una visión clara de lo que se espera.

Las áreas propietarias de los sistemas de información, en acompañamiento con la Oficina Coordinadora de Gestion de la Información deben establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad de la información.

Las áreas propietarias de los sistemas de información deben definir qué información sensible puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando estos ya no son requeridos.

Los desarrolladores deben documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

Los desarrolladores deben certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.

Los desarrolladores deben deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.

Los desarrolladores deben establecer el tiempo de duración de las sesiones activas de las aplicaciones, terminándolas una vez se cumpla este tiempo.

Los desarrolladores deben asegurar que no se permitan conexiones recurrentes a los sistemas de información construidos con el mismo usuario.

Los desarrolladores deben utilizar los protocolos sugeridos por la Oficina Coordinadora de Gestion de la Información en los aplicativos desarrollados.

Los desarrolladores deben certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por el hospital HUV.

Los propietarios de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de seguridad establecidos antes del paso a producción de los sistemas, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica en la cual funcionan los aplicativos.

Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

La Oficina Coordinadora de Gestion de la Información debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

La Oficina Coordinadora de Gestion de la Información debe contar con sistemas de control de versiones para administrar los cambios de los sistemas de información del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE.

La Oficina Coordinadora de Gestion de la Información debe asegurase que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

La Oficina Coordinadora de Gestion de la Información debe generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

La Oficina Coordinadora de Gestion de la Información, a través de sus funcionarios, se debe asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.

La Oficina Coordinadora de Gestion de la Información debe incluir dentro del procedimiento y los controles de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información del hospital HUV.

LINEAMIENTOS DE SEGURIDAD CON TERCEROS

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE en su interés por proteger su información y los recursos de procesamiento de la misma demostrará el compromiso de la Alta Gerencia en este esfuerzo, promoviendo que el personal cuente con el nivel deseado de conciencia en seguridad de la información para la correcta gestión de los activos de información y ejecutando el proceso disciplinario necesario cuando se incumplan laspolítica de seguridad de la información del hospital HUV.

Todos los funcionarios del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgos la seguridad y el buen nombre de la entidad.

La Alta Gerencia debe demostrar su compromiso con la seguridad de la información por medio de su aprobación de las políticas, normas y demás lineamientos que desee establecer el hospital HUV, en cabeza de la Oficina Coordinadora de Gestion de la Información.

La Alta Gerencia debe promover la importancia de la seguridad de la información entre los funcionarios del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE y el personal provisto por terceras partes, así como motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares para la seguridad de la información establecidos.

La Alta Gerencia debe definir y establecer el proceso disciplinario o incluir en el proceso disciplinario existente el hospital HUV, el tratamiento de las faltas de cumplimiento a laspolítica de seguridad o los incidentes de seguridad que lo ameriten.

La Gerencia Administrativa debe aplicar el proceso disciplinario del hospital HUV cuando se identifiquen violaciones o incumplimientos a laspolítica de seguridad de la información.

La Oficina de Recursos Humanos debe convocar a los funcionarios a las charlas y eventos programados como parte del programa de concientización en seguridad de la información, proveer los recursos para la ejecución de las capacitaciones y controlar la asistencia a dichas charlas y eventos, aplicando las sanciones pertinentes por la falta de asistencia no justificada.

Los funcionarios y personal provisto por terceras partes que por sus funciones hagan uso de la información del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, deben dar cumplimiento a las políticas, normas y procedimientos de seguridad de la información, así como asistir a las capacitaciones que sean referentes a la seguridad de la información.

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE asegurará que sus funcionarios y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas labores de una forma ordenada, controlada y segura.

La Oficina de Recursos Humanos debe realizar el proceso de desvinculación, licencias, vacaciones o cambio de labores de los funcionarios del hospital HUV llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

LINEAMIENTOS DE GESTION DE INCIDENTES

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE promoverá entre los funcionarios y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

La Alta Gerencia o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

La Oficina Coordinadora de Gestion de la Información debe establecer responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.

La Oficina Coordinadora de Gestion de la Información debe evaluar todos los incidentes de seguridad de acuerdo a sus circunstancias particulares y escalar al Comité de Seguridad aquellos en los que se considere pertinente.

La Oficina Coordinadora de Gestion de la Información debe designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y previniendo su reincidencia.

La Oficina Coordinadora de Gestión de la Información, con el apoyo de la Gerencia Administrativa, debe crear bases de conocimiento para los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros.

El Comité de Seguridad de la Información debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Es responsabilidad de los funcionarios del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

En caso de conocer la pérdida o divulgación no autorizada de información clasificada como uso interno, reservada o restringida, los funcionarios deben notificarlo a la Oficina Coordinadora de Gestion de la Información para que se registre y se le dé el trámite necesario.

Toda la información relativa a los incidentes reportados, debe ser manejada con total confidencialidad.

La Gerencia General del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, solicitará la asesoría legal para las acciones a realizar en incidentes relacionados con:

suplantación de identidad, acceso a información confidencial e incidentes relacionados con ingeniería social.

La Gerencia General del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE deberá aprobar un plan de continuidad de la seguridad de la información para reducir las interrupciones en las actividades misionales, como consecuencia de fallos o desastres que impidan su normal funcionamiento; el cual estará orientado a los procesos involucrados en las políticas, PSD, teniendo en cuenta la fase de análisis de riesgos.

La revisión del plan de contingencia de la seguridad de la información debe hacerse anualmente, dependiendo de los cambios y nuevos requerimientos en los procesos.

El Data Center se debe proveer con unidades suplementarias de energía eléctrica (UPS) y se debe garantizar el óptimo funcionamiento de ellas.

GESTIÓN DE RIESGOS

Las copias de seguridad de los sistemas de computación que incluye sistema operativo, base de datos, aplicación, servicios, entre otros; deben ser almacenados en un lugar diferente de donde reside la información original, dentro de las instalaciones del hospital HUV.

A los equipos servidores, de comunicaciones y demás dispositivos en los cuales haya configurados servicios debe realizársele un mantenimiento preventivo y periódico, de tal forma que el riesgo a fallas físicas se mantenga en una probabilidad de ocurrencia baja.

A intervalos programados se realizará mantenimiento preventivo a los equipos de cómputo de los usuarios finales, propiedad de la Institución, para reducir el riesgo de falla.

Los planes de contingencia deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse y sus resultados y las acciones de corrección deben comunicarse a la alta Gerencia.

LIENAMIENTOS DE CUMPLIMIENTO

El líder del proceso Gestión Jurídica tiene la responsabilidad de identificar la legislación vigente que debe cumplir el HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE en función de la protección de la información y divulgar estos requerimientos. Además, debe servir de apoyo en la interpretación, asistencia y manejo de dicha legislación.

Todos los funcionarios del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE deben cumplir con la normatividad vigente adoptada por el Hospital HUV, leyes de derechos de autor, acuerdos de licenciamiento de software y acuerdos de confidencialidad.

La Oficina Coordinadora de Gestion de la Información debe certificar que todo el software que se ejecuta en el Hospital HUV esté protegido por derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

La Oficina Coordinadora de Gestion de la Información debe establecer un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo o equipos móviles del Hospital HUV para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado en dichas estaciones de trabajo o equipos móviles corresponda únicamente al permitido.

Los usuarios no deben instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.

Los usuarios deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software. Es ilegal duplicar software o su documentación sin la autorización del propietario de los derechos de autor y, su reproducción no autorizada es una violación de ley; no obstante, puede distribuirse un número de copias bajo una licencia otorgada.

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, el HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE a través de la Oficina Asesora Jurídica, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales el HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que en algún momento, por razones de la actividad que desarrolla el Hospital HUV, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, el HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

Así mismo, buscará proteger la privacidad de la información personal de sus funcionarios, estableciendo los controles necesarios para preservar aquella información que el Hospital HUV conozca y almacene de ellos, velando porque dicha información sea utilizada únicamente para funciones propias del Hospital HUV y no sea publicada, revelada o entregada a funcionarios o terceras partes sin autorización.

Las áreas y servicios que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades del Hospital HUV.

Las áreas y servicios que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben asegurar que solo aquellas personas que tengan una necesidad laboral legítima puedan tener acceso a dichos datos.

Las áreas y servicios que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

Las áreas y servicios que procesan datos personales de beneficiarios, funcionarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados para el tratamiento de dichos datos personales.

Las áreas que procesan datos personales de beneficiarios, proveedores u otras terceras partes deben acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

La Oficina Coordinadora de Gestion de la Información debe implantar los controles necesarios para proteger la información personal de los beneficiarios, funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

Los usuarios deben guardar la discreción correspondiente, o la reserva absoluta con respecto a la información del Hospital HUV o de sus funcionarios de cual tengan conocimiento en el ejercicio de sus funciones.

Es deber de los usuarios, verificar la identidad de todas aquellas personas, a quienes se les entrega información por teléfono, por fax, por correo electrónico o por correo certificado, entre otros.

Los usuarios de los portales web e intranet del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE deben asumir la responsabilidad individual sobre la clave de acceso a dichos portales que les es suministrada; así mismo, deben cambiar de manera periódica esta clave de acceso.

Los usuarios de los portales web del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE deben contar con controles de seguridad en sus equipos de cómputo o redes privadas para acceder a la web.

Los usuarios de los portales web del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE deben aceptar el suministro de datos personales que pueda hacer el Hospital HUV a los terceros delegados para el tratamiento de datos personales, a entidades judiciales y demás entes del estado que, en ejercicio de sus funciones, solicitan esta información; de igual manera, deben aceptar que pueden ser objeto de procesos de auditoria interna o externa.

LINEAMIENTO DE CONTROL DE BACKUPS

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE certificará la generación de copias de respaldo y almacenamiento de su información crítica, proporcionando los recursos necesarios y estableciendo los procedimientos y mecanismos para la realización de estas actividades.

Las áreas propietarias de la información, con el apoyo de la Oficina Coordinadora de Gestion de la Información, encargada de la generación de copias de respaldo, definirán la estrategia a seguir y los periodos de retención para el respaldo y almacenamiento de la información.

Así mismo, el Hospital HUV velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

El personal asignado de la Oficina Coordinadora de Gestion de la Información debe respaldar con copias de seguridad la información Institucional que sea de misión crítica, dichas copias deben ser tomadas y probadas de acuerdo al procedimiento Control de Backups.

El personal asignado de la Oficina Coordinadora de Gestion de la Información debe garantizar copia de la información de configuración contenida en la plataforma tecnológica de la Institución como equipos tipo servidores, equipos activos de red, dispositivos de red inalámbricos, y software que administre, dichas copias deben ser tomadas y probadas.

Los medios magnéticos que tienen información crítica deben ser almacenados en otra ubicación diferente a las instalaciones donde se encuentra ubicada. El sitio externo donde se resguardan dichas copias, solo tendrá acceso el personal asignado de la Oficina Coordinadora de Gestion de la Información.

La Oficina Coordinadora de Gestion de la Información, a través de sus funcionarios, debe generar y adoptar los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

La Oficina Coordinadora de Gestion de la Información debe disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

La Oficina Coordinadora de Gestion de la Información, a través de sus funcionarios, debe llevar a cabo los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

La Oficina Coordinadora de Gestion de la Información debe definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

La Oficina Coordinadora de Gestion de la Información debe proporcionar apoyo para la definición de las estrategias de generación, retención y rotación de las copias de respaldo de la los activos información del Hospital HUV.

Los propietarios de los recursos tecnológicos y sistemas de información deben definir, en conjunto con la Oficina Coordinadora de Gestion de la Información, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Es responsabilidad de los usuarios de la plataforma tecnológica del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE identificar la información crítica que debe ser respaldada y almacenarla de acuerdo con su nivel de clasificación.

GENERALIDADES: En este documento se elaborarán las política de seguridad con el propósito de proteger la información del hospital HUV, las cuales serán la base para la implementación de las medidas de seguridad que contribuirán a mantener la integridad, confidencialidad y disponibilidad de los datos dentro de los sistemas.

Este documento da a conocer una serie depolítica para tener en cuenta en el momento de realizar una copia de respaldo (Backups), el cual depende de los recursos disponibles como de las necesidades de respaldo dentro de la institución.

Los procedimientos de respaldo y recuperación son procedimientos críticos e importantes y ayudan a prevenir posibles desastres ante fallas de los equipos, falla de energía, borrado accidental de archivos, caída del sistema, etc.

DEFINICION: Una política de seguridad de información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y su integridad.

ALCANCE: Esta política es de aplicación en el conjunto de dependencias que componen la institución, a sus recursos, a la totalidad de los procesos internos o externos vinculados al hospital a través de contratos o acuerdos con terceros y a todo el personal del HUV, cualquiera sea su situación contractual, la dependencia a la cual se encuentre adscrito y el nivel de las tareas que desempeña.

OBJETIVO: Proteger, preservar y administrar la información, las bases de datos y toda la documentación critica al interior del HUV junto con las tecnologías utilizadas para su

procesamiento, frente a amenazas internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de los características de confidencialidad, integridad, disponibilidad, legalidad, y confiabilidad de la información.

RESPONSABILIDADES: Es responsabilidad de los administradores de los servidores de la Oficina Coordinadora de Gestion de la Información (Comité de Seguridad) conocer, adoptar e implementar la presente política de Backups; también son los responsables de mantener actualizadas laspolítica y procedimientos.

La Política de Copias de Respaldo o Backups de la Información es de aplicación obligatoria para todo el personal del HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE, cualquiera sea su situación contractual, la dependencia a la que pertenezca y el nivel de las tareas que desempeñe.

TIPOS DE RESPALDO: Una copia de respaldo incremental sólo copia los datos que han variado desde la última operación de Backups de cualquier tipo. Se suele utilizar la hora y fecha de modificación estampada en los archivos, comparándola con la hora y fecha del último Backups.

Como un Backups incremental sólo copia los datos a partir del último Backups de cualquier tipo, se puede ejecutar tantas veces como se desee, pues sólo guarda los cambios más recientes. La ventaja de un Backups incremental es que copia una menor cantidad de datos que un Backups completo. Por ello, esas operaciones se realizan más deprisa y exigen menos espacio para almacenar la copia.

DISPOSITIVOS: Existen ciertas condiciones con las que se deben guardar los respaldos, con el fin de garantizar una adecuada conservación de la información. A continuación se indican las condiciones que se deben tener en cuenta para el óptimo funcionamiento de los dispositivos:

- La humedad relativa del ambiente se debe encontrar entre el 20 % al 80 %, La temperatura puede oscilar entre 5°C a 45°C.
- El ambiente debe contar con aire acondicionado o ventilación.
- Los dispositivos deben mantenerse alejados de campos magnéticos.

Para realizar un respaldo se debe contar como mínimo con un dispositivo de almacenamiento externo, este puede ser, una cinta o disco removible. Si no se cuenta con un dispositivo de almacenamiento externo es recomendable utilizar al menos y de manera temporal el disco duro de otra máquina. Esta es una medida temporal mientras se adquiere un dispositivo de almacenamiento externo más seguro para aplicar el procedimiento de respaldos correctamente.

Es recomendable contar con un sitio externo a la institución para guardar algunas copias de respaldos semestrales, como contingencia en caso de desastre. Entre los soportes más habituales, podemos destacar las cintas magnéticas, discos compactos o cualquier dispositivo capaz de almacenar los datos que se pretenden salvaguardar.

APLICACIÓN: El administrador del servidor deberá plasmar los procedimientos para el respaldo y recuperación, antes de entrar en producción el servidor. Los mismos serán controlados por el administrador de la aplicación, para verificar que es clara y completa, los procedimientos deberán contemplar como mínimo los siguientes elementos:

- El sistema operativo de los servidores y su configuración
- Los parches y paquetes de software de base necesarios para que la aplicación se ejecute
- Los programas que componen la aplicación
- Los archivos y/o bases de datos del sistema
- Horario de ejecución de la copia de respaldo

Todas las copias de respaldo deberán estar claramente identificadas, con etiquetas que indiquen como mínimo:

- Número de secuencia
- Tipo de Backups
- Nombre del sistema o aplicativo
- Datos necesarios para su reconocimiento
- Equipo al que pertenece
- Fecha y hora de ejecución
- Frecuencia

Todos los procedimientos de respaldo deberán generar un registro en el sistema de Backups que permita la revisión del resultado de la ejecución.

Queda estrictamente prohibido almacenar, en las carpetas a las cuales se les va a realizar el respaldo, archivos de juegos, música, reproductores de música y/o video, programas de cómputo sin licencia y cualquier otra información ajena a la Institución.

Se efectuarán pruebas de recuperación de las copias de respaldo por parte del administrador del sistema de Backups cada semestre y serán supervisadas por el administrador del servidor. Con esto se podrá evidenciar que los datos grabados en los dispositivos se pueden obtener correctamente al momento de ser necesarios. Las pruebas se deberán formalizar en un acta escrita y firmada por los responsables.

Los procedimientos de generación y grabación de estos archivos serán automáticos, con el fin de evitar su modificación.

PERIODICIDAD: Las copias de respaldo o Backups realizados por los usuarios de las diferentes áreas del Hospital HUV deberán estar sujetas a la normatividad estipulada en la tabla de retención documental (TRD).

Se llevará un registro semanal de los dispositivos en uso indicando como mínimo:

- Fecha de ejecución del respaldo
- Dispositivos (Discos) que integran el Backups de los equipos
- Cantidad de veces que usa el dispositivo (disco). Luego deberá procederse a su respectivo cambio.
- Los discos de Backups se almacenarán en un lugar bajo llave con las condiciones ambientales descritas en la política.
- El administrador del sistema de Backups revisará periódicamente que se cumpla con este registro en tiempo y forma.

MÉTODO EMPLEADO: En caso de utilizar Backups de solo datos, esto aplica para los usuarios de las distintas dependencias del Hospital HUV, se deberá tener en cuenta lo siguiente:

- Se documentará la secuencia de los dispositivos, cintas o discos usados.
- Deberán existir controles para prevenir el uso excesivo de la vida útil de dispositivos.
- Se realizará un Backups de los datos cada 7 días.

En caso de utilizar Backups incremental (Subgerencia Gestión de la Información) se deberá tener en cuenta lo siguiente:

- Se documentará la identificación de secuencia de los Backups incrementales.

- Deberán existir controles para prevenir la carga de dispositivos (cintas o discos) en una secuencia equivocada.
- Se realizará un Backups del sistema completo cada 15 días.

DESTRUCCIÓN DEL BACKUP: La información en un medio de respaldo será destruida de dos formas:

Reutilización del medio para otro uso: El encargado de la administración y manejo de los Backups deberá tener definido un rol para la reutilización de los medios, para esto debe llevar el control del contenido actual de cada respaldo. Cuando se reutilice el dispositivo se debe actualizar la información del medio.

Daño físico del medio de respaldo: Deberán hacerse en forma periódica pruebas de restauraciones de información en un área temporal con el fin de probar el buen estado del medio de respaldo. Si se comprueba que el medio tiene un daño y no puede leerse su contenido, se debe destruir físicamente y documentar el número de dispositivo y su último contenido. Se debe tratar que rescatar la mínima cantidad de información y guardarla en otro medio.

LINEAMIENTOS PARA LA ADQUISICION DE BIENES DE INFORMATICA

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 Oficina Coordinadora de Gestión de la Información.

Toda adquisición de tecnología informática de impacto se efectúa a través de la Oficina Coordinadora de Gestion 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 Oficina Coordinadora de Gestion 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 HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” E.S.E., la Oficina Coordinadora de Gestion 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 HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” 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 Oficina Coordinadora de Gestion 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 Oficina Coordinadora 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.

7. ACCIONES DE CONTINGENCIA

El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE proporcionará los recursos suficientes para proporcionar una respuesta efectiva de funcionarios y procesos en caso de contingencia o eventos catastróficos que se presenten en el Hospital HUV y que afecten la continuidad de su operación.

Además, responderá de manera efectiva ante eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. El HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” ESE mantendrá canales de comunicación adecuados hacia funcionarios, proveedores y terceras partes interesadas.
La Oficina Coordinadora de Gestion de la Información, en conjunto con la Brigada de Emergencias y/o Comité Hospitalario de Emergencias, deben elaborar un plan de recuperación ante desastres para el centro de cómputo y un conjunto de procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados.
La Oficina Coordinadora de Gestion de la Información y la Gerencia Administrativa deben participar activamente en las pruebas de recuperación ante desastres y notificar los resultados al Comité Hospitalario de Emergencias y/o Gerencia General.
La Oficina Coordinadora de Gestion de la Información y cada área operativa creará para la Institución y sus departamentos un plan de contingencias informáticas que incluya al menos los siguientes puntos:

- Continuar con la operación de la unidad administrativa con procedimientos informáticos alternos.
- Tener los respaldos de información en un lugar seguro, fuera del lugar en el que se encuentran los equipos.
- Tener el apoyo por medios magnéticos o en forma documental, de las operaciones necesarias para reconstruir los archivos dañados.
- Contar con un instructivo de operación para la detección de posibles fallas, para que toda acción correctiva se efectúe con la mínima degradación posible de los datos.
- Contar con un directorio del personal interno y del personal externo de soporte, al cual se pueda recurrir en el momento en que se detecte cualquier anomalía;
- Ejecutar pruebas de la funcionalidad del plan.
- Mantener revisiones del plan a fin de efectuar las actualizaciones respectivas.
- Redundancia en el sistema de Internet mediante el uso de dos ISP con ingreso al edificio de la institución por dos rutas diferentes.
- Uso de sistema de extinción de incendios especializado en sistemas electrónicos de alta sensibilidad en el data center.
- Uso de fuentes redundantes para el núcleo de servidores.

La Gerencia General del Hospital HUV deberá aprobar un plan de continuidad de la seguridad de la información para reducir las interrupciones en las actividades misionales, como consecuencia

de fallos o desastres que impidan su normal funcionamiento; el cual estará orientado a los procesos involucrados en la PSD, teniendo en cuenta la fase de análisis de riesgos.
La revisión del Plan de Continuidad de la seguridad de la información debe hacerse anualmente, dependiendo de los cambios y nuevos requerimientos en los procesos.
El Data Center se debe proveer con unidades suplementarias de energía eléctrica (UPS) y se debe garantizar el óptimo funcionamiento de dichas unidades.
Las copias de seguridad de los sistemas de computación que incluye sistema operativo, base de datos, aplicación, servicios, entre otros; deben ser almacenados en un lugar diferente de donde reside la información original, dentro de las instalaciones del Hospital HUV.
A los equipos servidores, de comunicaciones y demás equipos en los cuales haya configurados servicios debe realizársele un mantenimiento preventivo y periódico, de tal forma que el riesgo a fallas físicas se mantenga en una probabilidad de ocurrencia baja.
A intervalos programados se realizará mantenimiento preventivo a los equipos de cómputo de los usuarios finales, propiedad de la Institución, para reducir el riesgo de falla.
Los planes de continuidad deben ser probados regularmente con el fin de asegurar que el plan sea relevante, efectivo, práctico y factible de realizar. Cada prueba debe documentarse, sus resultados y las acciones de corrección deben comunicarse a la alta Gerencia.
La Institución gestiona y ejecuta los planes de capacitación para garantizar la formación y actualización de los funcionarios de la Oficina Coordinadora de Gestion de la Información conforme a las necesidades de modernización tecnológica que se presenten y mantener la confidencialidad, disponibilidad e integridad de los diferentes activos de información de la institución, así como la continuidad en la prestación de servicios de la plataforma tecnológica.
Los Subgerentes, Directores y Jefes de Áreas deben identificar y, al interior de sus áreas, generar la documentación de los procedimientos de continuidad que podrían ser utilizados en caso de un evento adverso, teniendo en cuenta la seguridad de la información. Estos documentos deben ser probados para certificar su efectividad.
Para la Oficina Coordinadora de Gestion de la Información, los planes de contingencia, son:

PLAN DE PREVENCION EVENTO INCENDIO

a. Descripción del evento: Es un proceso de combustión caracterizado por la emisión de calor acompañado de humo, llamas o ambas que se propaga de manera incontrolable en el tiempo y en el espacio. Se producen en materiales sólidos, líquidos combustibles inflamables, equipos e instalaciones bajo carga eléctrica entre otros.
b. Objetivo: Establecer las acciones que se ejecutaran ante un incendio a fin de minimizar el tiempo de interrupción de las operaciones de la institución sin exponer la seguridad de las personas.
c. Criticidad: La Subgerencia Gestión de la Información determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.
d. Entorno: Este evento se puede dar en las instalaciones de la Subgerencia Gestión de la Información del HUV.
e. Personal Encargado: El Subgerente Gestión de la Información, es quien debe dar cumplimiento a lo descrito en las condiciones de prevención de riesgo del presente plan.
f. Condiciones de Prevención de Riesgo:

- Realizar inspecciones de seguridad periódicamente.
- Mantener las conexiones eléctricas seguras en el rango de su vida útil.
- Realizar charlas y prácticas sobre el uso y manejo de los diferentes tipos de extintores.
- Acatar las indicaciones de la Brigada de Emergencias del Hospital.
- Contar con una agenda de teléfonos que incluya a los bomberos, ambulancias, Comité Hospitalario de Emergencias y personal del HUV.
- Responsable de las acciones de prevención y ejecución de la contingencia.

- Contar con los elementos necesarios para la detección y extinción de un posible incendio, los cuales cubran los ambientes del “Centro de Datos” y áreas afines a la Subgerencia Gestión de la Información.
- Mantener actualizado los extintores con SOLKAFLAM y el equipo FM-200 FIRE SUPPRESION SYSTEM.

PLAN DE EJECUCION

a. Eventos que activan la contingencia:
La Contingencia se activará al ocurrir un incendio.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.
b. Procesos relacionados antes del evento:
Identificar la ubicación de las estaciones manuales de alarma contra incendio.
Identificar la ubicación de los extintores.
Conocer el número de teléfono del Comité Hospitalario de Emergencias, del personal responsable en seguridad Informática, de contingencia del HUV., de la Brigada de Emergencias y de Bomberos.
c. Personal que autoriza la contingencia: El Gerente Administrativo, Subgerente Gestión de la Información o sus Representantes pueden activar la contingencia.
d. Descripción de las actividades después de activar la contingencia:

- Tratar de apagar el incendio con extintores.
- Comunicar al personal responsable del Comité Hospitalario de Emergencias.
- Evacuar el Área.
- En todo momento se coordinara con el Comité de Contingencia y Seguridad, para las acciones que deban ser efectuadas por ellos.
- Luego de extinguido el incendio, se deberán realizar las siguientes actividades:
- Evaluación de los daños ocasionados al personal, bienes e instalaciones.
- En caso de daños del personal prestar asistencia médica inmediata
- Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
- En caso de que se hayan detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.
- La Coordinación Ejecutora del Plan de Contingencias deberá acordar con la Alta Gerencia del HUV, en caso de que se requiera la habilitación de espacios provisionales alternos para restablecer la función de los ambientes afectados.

e. Duración: La duración de la contingencia dependerá del tiempo que demande controlar el incendio.
f. DRP: este evento es de alto impacto y por consiguiente debe estar incluido en el DRP.
g.Equipo de trabajo: Todo el personal de la Oficina Coordinadora de Gestion de la Información, especialmente el Administrador de Infraestructura, el DBA, Área de redes y Área de soporte técnico.

PLAN DE RECUPERACION

a. Personal Encargado: El personal encargado del plan de recuperación es la Gerencia Administrativa y la Oficina Coordinadora de Gestion de la Información, cuyo rol principal es asegurar el normal desarrollo de las operaciones en el HUV.
b. Descripción: El plan de recuperación estará orientado a restablecer en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.
c. Mecanismos de Comprobación: El Subgerente de Gestión de la Información presentará un informe a la Coordinación Ejecutora del Plan explicando que parte de las actividades u operaciones han sido afectadas y cuáles son las acciones a seguir.

d. Mecanismos de Recuperación: Se efectuara de acuerdo a las instrucciones impartidas por el personal encargado del plan.

A.Adaptación del espacio provisional alterno donde se instalaran servidores, switchs y toda la infraestructura de tecnología necesaria, para conectar y habilitar toda la red de computadores del hospital.

b. La restauración de las copias de respaldo que facilite la puesta en marcha del negocio y el reinicio de las labores en el menor tiempo posible.

e . Desactivación del Plan de Contingencia: El Gerente Administrativo, Subgerente Gestión de la Información o sus representantes desactivarán el plan de contingencia una vez que se hayan realizado las acciones descritas en el presente plan, mediante una comunicación a la Coordinación Ejecutora del Plan.

f. Proceso de Actualización: El proceso de Actualización será con base al informe presentado por el Gerente Administrativo y/o Subgerente Gestión de la Información luego de lo cual se determinarán las acciones a tomar.

PLAN DE PREVENCION EVENTO SISMO

a. Descripción del evento: Los sismos son movimientos en el interior de la tierra y que generan una liberación repentina de energía que se propaga en forma de ondas provocando el movimiento del terreno. Este evento incluye los siguientes elementos mínimos identificados por la Subgerencia Gestión de la Información, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

b.Objetivo: Establecer las acciones que se tomaran ante un sismo a fin de minimizar el tiempo de interrupción de las operaciones del HUV., evitando exponer la seguridad de las personas.

c. Criticidad: La Subgerencia Gestión de la Información del HUV., determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.

d. Entorno: Este evento se puede dar en las instalaciones de la Subgerencia Gestión de la Información del HUV.

e. Personal Encargado: El Subgerente Gestión de la Información del HUV, es quien debe dar cumplimiento a lo descrito en las condiciones de prevención de riesgo del presente plan.

f. Condiciones de Prevención del Riesgo:

Contar con un plan de evacuación de las instalaciones del HUV. El cual debe ser de conocimiento de todo el personal.

Realizar simulacros de evacuación con la participación de todo el personal del HUV.

Mantener las salidas libres de obstáculos.

Señalizar todas las salidas.

Señalizar las zonas seguras.

PLAN DE EJECUCION

a. Eventos que activan la Contingencia:

La Contingencia se activará al ocurrir un sismo

El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b. Procesos Relacionados antes del evento:

Tener la lista de los empleados de la Oficina Coordinadora de Gestion de la Información.

Mantenimiento del orden y limpieza.

Inspecciones diarias de seguridad interna.

Inspecciones trimestrales de seguridad externa.

Realización de simulacros internos en horarios que no afecten las actividades

c. Personal que autoriza la contingencia: El Gerente Administrativo, el Subgerente Gestión de la Información o sus representantes pueden activar la contingencia.

d. Descripción de las actividades después de activar la contingencia:

Desconectar el fluido eléctrico y cerrar las llaves de gas u otros líquidos inflamables si corresponde.

Evacuar las oficinas de acuerdo a las disposiciones del Gerente Administrativo y/o Subgerente Gestión de la Información utilizando las rutas establecidas durante los simulacros. Considerar las escaleras de emergencia, señalización de rutas, zonas de agrupamiento del personal, etc.
Por ningún motivo utilizar los ascensores, mantener la calma, evitar pánico y circular por la derecha.
Verificar que todo el personal que labora en el área se encuentre bien.
Brindar los primeros auxilios al personal afectado si fuese necesario.
Alejarse de las ventanas para evitar sufrir cortes por roturas y/o desprendimiento de trozos de vidrio.
Evaluación de los daños ocasionados por el sismo sobre las instalaciones físicas, ambientes de trabajo, estanterías, instalaciones eléctricas, documentos, etc. En caso de requerirse personal especializado (Bomberos), acordar su presencia a través de la Coordinación Ejecutora del Plan de Contingencias.
Inventario general de la documentación, del personal, de los equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
Limpieza de las áreas afectadas por el sismo.
En todo momento se coordinará con personal de mantenimiento del HUV., para las acciones que deban ser efectuadas por ellos.
La Coordinación Ejecutora del Plan de Contingencias deberá acordar con la Alta Gerencia del HUV. En caso de que se requiera la habilitación de espacios provisionales alternos para restablecer la función de los ambientes afectados.
e. Duración: Los procesos de evacuación del personal del HUV. deberán efectuarse de forma calmada, transitando por la derecha, evitando el pánico y demorarán 5 minutos como máximo. La duración total del evento dependerá del grado del sismo, de la probabilidad de réplicas y de los daños presentados en la infraestructura.
f. DRP: este evento es de carácter externo, de alto impacto y por consiguiente debe estar incluido en el DRP.
g. Equipo de trabajo: Todo el personal de la Oficina Coordinadora de Gestion de la Información.

PLAN DE RECUPERACION

a. Personal Encargado: El personal encargado del plan de recuperación es el Gerente Administrativo y/o el Subgerente de Gestión de la Información del HUV, cuyo rol principal es asegurar el normal desarrollo de las operaciones de la Institución.
b. Descripción: El plan de recuperación estará orientado a recuperar en el menor tiempo posible la producción y puesta en marcha pendiente durante la interrupción del servicio.
c. Mecanismos de Comprobación: El Gerente Administrativo y/o Subgerente de Gestión de la Información presentará un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio u operaciones han sido afectadas y cuáles son las acciones a seguir.
d. Mecanismos de Recuperación: Se efectuará de acuerdo a las instrucciones impartidas por el personal encargado del plan.
A. Adaptación del espacio provisional alterno donde se instalarán servidores, switchs y toda la infraestructura de tecnología necesaria, para conectar y habilitar toda la red de computadores del hospital.
b. La restauración de las copias de respaldo que facilite la puesta en marcha del negocio y el reinicio de las labores en el menor tiempo posible.
c. Desactivación del Plan de Contingencia: El Gerente Administrativo y/o Subgerente Gestión de la Información desactivaran el Plan de Contingencia una vez que se haya tomado las acciones descritas en la descripción del presente plan de recuperación, mediante una comunicación escrita y/o electrónica a la Coordinación Ejecutora del Plan.
d. Proceso de Actualización: El proceso de actualización será con base al informe presentado por el Gerente Administrativo y/o Subgerente Gestión de la Información quien determinará las acciones a tomar.

PLAN DE PREVENCION EVENTO INTERRUPCIÓN DE SUMINISTRO ENERGIA ELECTRICA

a. Descripción del evento: Falla general del suministro de energía eléctrica.

Este evento incluye los siguientes elementos mínimos identificados por la Subgerencia Gestión de la Información, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

b. Objetivo: Restaurar las funciones consideradas como críticas para el servicio.

c.Criticidad: Este evento se considera como MEDIO.

d. Entorno: Se puede producir durante la operatividad, afectando el fluido eléctrico de las instalaciones del Data Center ubicado en la Subgerencia Gestión de la Información.

e. Personal encargado: El Subgerente de Gestión Técnica y/o el Subgerente de Gestión de la Información, son responsables de realizar las coordinaciones para restablecer el suministro de energía eléctrica.

f. Condiciones de Prevención de Riesgo:

Durante las operaciones diarias del servicio u operaciones del Data Center se contará con las UPS necesarias para asegurar el suministro eléctrico en las estaciones de trabajo consideradas como críticas.

Asegurar que los equipos UPS cuenten con el mantenimiento debido y con suficiente energía para soportar una operación continua de 4 horas máximo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.

Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento.

Contar con UPS para proteger los servidores de correo y misión crítica, previniendo la perdida de datos durante las labores. La autonomía del equipo UPS no deberá ser menor a 30 minutos.

Contar con UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones del Data Center (puertas, contactos magnéticos, acceso biométrico etc.)

Contar con procedimientos operativos alternos para los casos de falta de sistemas, de tal forma que no se afecten considerablemente las operaciones en curso.

PLAN DE EJECUCION

a. Eventos que activan la contingencia: Corte de suministro de energía eléctrica en los ambientes del Data Center.

b. Procesos relacionados antes del evento: Cualquier actividad de servicio dentro de las instalaciones del HUV.

c. Personal que autoriza la contingencia: El Gerente Administrativo y/o el Subgerente de Gestión de la Información y/o Subgerente de Gestión Técnica, pueden activar la contingencia.

d. Descripción de los procedimientos después de activar la contingencia:

Informar al Gerente Administrativo y/o Subgerente Gestión de la Información y/o Subgerente Gestión Técnica del problema presentado.

Dar aviso del corte de energía eléctrica en forma oportuna a todas las áreas del HUV. y coordinar las acciones necesarias.

Las actividades afectadas por la falta de uso de aplicaciones, deberán iniciar sus procesos de contingencia a fin de no afectar las operaciones en curso.

En el caso de los equipos que entren en funcionamiento automático con UPS, se deberá monitorear el tiempo de autonomía del equipo y no exceder el indicado anteriormente.

e. DRP: este evento es de carácter interno y externo, de alto impacto y por consiguiente debe estar incluido en el DRP.

f.Equipo de trabajo: Todo el personal de la Oficina Coordinadora de Gestion de la Información.

PLAN DE RECUPERACION

a. Personal Encargado: El personal encargado del plan de recuperación son: el Subgerente Gestión de la Información y/o el Subgerente Gestión Técnica, quienes se encargaran de realizar las acciones de recuperación necesarias.

b. Descripción: El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos. Se informará a la Coordinación Ejecutora del Plan, el problema presentado y el procedimiento usado para atender el problema. En función a esto, se tomarán las medidas preventivas del caso.
c. Mecanismos de Comprobación: El Subgerente Gestión Técnica y/o Subgerente Gestión de la Información presentarán un informe a la Coordinación Ejecutora del Plan explicando que parte del Servicio u operaciones han fallado y cuáles son las acciones correctivas y/o preventivas a realizar.
d.Mecanismos de Recuperación: Se efectuara de acuerdo a las instrucciones impartidas por el personal encargado del plan.
a. Instalación de plantas eléctricas y baterías de larga duración, que permitan conectar y habilitar toda la red de computadores del hospital.
b. Reposición de equipos de cómputo y de redes de ser necesario.
c. Ante la pérdida de información: La restauración de las copias de respaldo que facilite la puesta en marcha del negocio y el reinicio de las labores en el menor tiempo posible.
e. Desactivación del Plan de Contingencia: El Subgerente Gestión Técnica y/o Subgerente Gestión de la Información desactivarán el plan de contingencia una vez que se recupere la funcionalidad de trabajo con todos los sistemas.
f. Proceso de Actualización: Con base al informe que describe los problemas presentados, se determinaran las acciones de prevención a tomar.

PLAN DE PREVENCION EVENTO INFECCION DE EQUIPOS POR VIRUS

Descripción del evento: Virus informático es un programa de software que se propaga de un equipo a otro y que interfiere el funcionamiento del pc. Además, Un virus informático puede dañar o eliminar los datos de un servidor o un computador, basados en el sistema operativo Windows en todas sus versiones.
Este evento incluye los siguientes elementos mínimos identificados por la Subgerencia Gestión de la Información, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:
Hardware Software
Servidores Software base
Estaciones de trabajo Aplicativos utilizados en el HUV
a. Objetivo: Restaurar la operatividad de los servidores después de eliminar los virus o reinstalar las aplicaciones dañadas.
b. Criticidad: El nivel de este evento es considerado CRÍTICO.
c. Entorno: Los servidores o equipos de trabajo que se encuentren instalados al interior del edificio Hospital Universitario del Valle dispersos en sus siete pisos de estructura física.
d. Personal Encargado: El Subgerente Gestión de la Información y/o Soporte Técnico de Sistemas son los responsables en la supervisión del correcto funcionamiento de las estaciones de trabajo y Pc´s
e. Condiciones de Prevención de Riesgo:
Establecimiento depolítica de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
Restringir el acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
Eliminación de quemadores de CD, etc. en estaciones de trabajo que no lo requieran.
Deshabilitar los puertos de comunicación USB en las estaciones de trabajo que no los requieran, para prevenir la conexión de unidades de almacenamiento externo.
Aplicar filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo.
Contar con antivirus instalado y actualizado en cada estación de trabajo que utilice el Sistema Operativo Windows, el mismo que debe estar actualizado permanentemente.
Contar con equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta su desinfección y habilitación.

PLAN DE EJECUCION

a. Eventos que activan la contingencia:
Mensajes de error durante la ejecución de programas.
Lentitud en el acceso a las aplicaciones.
Falla general en el equipo (sistema operativo, aplicaciones).

b. Procesos relacionados antes del evento: Cualquier proceso relacionado con el uso de las aplicaciones en las estaciones de trabajo.

c. Personal que autoriza la contingencia: El Subgerente Gestión de la Información y/o Soporte Técnico de Sistemas.

d. Descripción de las Actividades después de activar la contingencia:
Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.
Desconectar la estación infectada de la red del HUV.
Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.)
Eliminar el agente causante de la infección.
Remover el virus del sistema.
Probar el sistema.
En caso de no solucionarse el problema:
Formatear el equipo
Personalizar la estación para el usuario
Conectar la estación a la red del HUV.
Efectuar las pruebas necesarias con el usuario.
Solicitar conformidad del servicio.

e. Duración: La duración del evento no deberá ser mayor a dos horas en caso de que se confirme la presencia de un virus. Esperar la indicación del personal de soporte para reanudar el trabajo.

f. DRP: este evento es de carácter interno, de alto impacto y por consiguiente debe estar incluido en el DRP.

g. Equipo de trabajo: Todo el personal de la Oficina Coordinadora de Gestion de la Información.

PLAN DE RECUPERACION

a. Personal Encargado: El Técnico de Soporte de Sistemas de la Oficina Coordinadora de Gestion de la Información del HUV, luego de restaurar el correcto funcionamiento de la estación de trabajo (Pc), coordinará con el usuario responsable y/o Jefe del área para reanudar las labores de trabajo con el equipo.

b. Descripción: Se informará al Subgerente Gestión de la Información del HUV, el tipo de virus encontrado y el procedimiento usado para removerlo. En función a esto, se tomaran las medidas preventivas del caso enviando una alerta vía correo al personal del HUV. El evento será evaluado y registrado de ser necesario en el formato de ocurrencia de eventos.

c. Mecanismos de Comprobación: Se llenará el formato de ocurrencia de eventos y se remitirá a la Coordinación Ejecutora del Plan para su revisión.

d. Mecanismos de Recuperación: Se efectuará de acuerdo a las instrucciones impartidas por el personal encargado del plan.
Desconectar el equipo o los equipos infectados de la red de información.
Realizar diagnostico técnico del software del equipo o de los equipos.
Instalar y escanear un programa antivirus en el equipo o los equipos afectados.
Ante la pérdida de información: La restauración de copias de respaldo y pruebas con el usuario.
Si hay daño del sistema operativo: reinstalación del mismo y de las copias de respaldo.

e. Desactivación del Plan de Contingencia: Con el aviso del Técnico de Soporte de Sistemas de la Oficina Coordinadora de Gestion de la Información del HUV, se desactivará el presente plan.

f. Proceso de Actualización: El problema de infección presentado en la estación de trabajo, no debe detener la actualización de datos en las aplicaciones del HUV.

PLAN DE PREVENCION EVENTO FILTRACION DE AGUA

a. Descripción del evento: Es un evento caracterizado por la caída de agua sobre el rack de los servidores, de los switches, causando chispas eléctricas, lo que puede originar un corto eléctrico, emisión de calor, humo, llamas y descargas eléctricas sobre pisos mojados y que se puede propagar rápidamente a través del cableado tanto de energía como de datos.
b. Objetivo: Establecer las acciones que se ejecutaran ante una caída de agua y el posible origen de un corto circuito a fin de minimizar el tiempo de interrupción de las operaciones de la institución sin exponer la seguridad de las personas.
c. Criticidad: La Subgerencia Gestión de la Información determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO.
d. Entorno: Este evento se puede dar en las instalaciones de la Subgerencia Gestión de la Información del HUV, en el área del Data Center.
e. Personal encargado: El Subgerente Gestión de la Información, es quien debe dar cumplimiento a lo descrito en las condiciones de prevención de riesgo del presente plan.
f. Condiciones de Prevención de Riesgo:
Realizar inspecciones de seguridad periódicamente.
Acatar las indicaciones de la Brigada de Emergencias del HUV.
Contar con una relación de teléfonos de emergencia que incluya a los bomberos, ambulancias, y personal del HUV.
Responsable de las acciones de prevención y ejecución de la contingencia.

PLAN DE EJECUCION

a. Eventos que activan la contingencia:
La Contingencia se activará al ocurrir una caída de agua.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.
b. Procesos relacionados antes del evento:
Identificar el sitio donde se guarde material aislante e impermeable
Conocer el número de teléfono del Comité Hospitalario de Emergencias, del personal responsable en seguridad Informática, de contingencia del HUV., de la Brigada de Emergencias y de Bomberos.
c. Personal que autoriza la contingencia: El Subgerente Gestión de la Información del HUV., o sus representantes pueden activar la contingencia.
Descripción de las actividades después de activar la contingencia:
Cerrar la llave de paso de los ductos de agua del piso que está ocasionando el daño
Tratar de sellar la entrada de agua en el Data Center.
Cubrir los equipos con elementos aislantes e impermeables
Tratar de apagar el fuego con extintores, si este se presenta
Comunicar al personal responsable del Comité Hospitalario de Emergencias y de la Brigada de Emergencias del HUV.
Luego de solucionado el evento, se deberán realizar las siguientes actividades:
Evaluación de los daños ocasionados a los bienes y a las instalaciones.
En caso de daños o traumas al personal prestar asistencia médica inmediata
Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
En caso de que se hayan detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.
La Coordinación Ejecutora del Plan de Contingencias deberá acordar con la Alta Gerencia del HUV., en caso de que se requiera la habilitación de espacios provisionales alternos para restablecer la función de los ambientes afectados.
d. Duración: La duración de la contingencia dependerá del tiempo que demande controlar la inundación o caída de agua y en el evento de haberse producido problemas eléctricos.
e. DRP: este evento es de carácter interno, de alto impacto y por consiguiente debe estar incluido en el DRP.

f. Equipo de trabajo: Todo el personal de la Oficina Coordinadora de Gestion de la Información.

PLAN DE RECUPERACION

a. Personal Encargado: El personal encargado del plan de recuperación es la Oficina Coordinadora de Gestion de la Información, cuyo rol principal es asegurar el normal desarrollo de las operaciones del HUV.

b. Descripción: El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

c. Mecanismos de Comprobación: El Subgerente de Gestión de la Información presentará un informe a la Gerencia Administrativa explicando que parte de las actividades u operaciones ha sido afectada y cuáles son las acciones a seguir.

d. Mecanismos de Recuperación: Se efectuara de acuerdo a las instrucciones impartidas por el personal encargado del plan:

Revisar que no hallan filtraciones de agua.

Revisar y constatar que todos los equipos afectados se encuentren totalmente secos.

Prender los equipos de cómputo, revisando que se encuentren operando perfectamente.

Ante algún daño, realizar su reposición y configuración.

Si hay pérdida de información, realizar restauración de copias de respaldo.

e. Desactivación del Plan de Contingencia: El Subgerente Gestión de la Información o sus representantes desactivarán el plan de contingencia una vez que se hayan tomado las acciones descritas en la descripción del presente plan de recuperación, mediante una comunicación a la Coordinación Ejecutora del Plan.

f. Proceso de Actualización: El proceso de Actualización será con base al informe presentado por el Subgerente Gestión de la Información, luego de lo cual se determinaran las acciones a seguir.

PLAN DE PREVENCION EVENTO VANDALISMO

a. Descripción del evento: Es un proceso mediante el cual una persona o un grupo de individuos atacan y destruyen instalaciones, equipos, archivos, documentación pertenecientes a una empresa o una área específica.

b. Objetivo: Establecer las acciones que se ejecutaran ante un ataque de vandalismo a fin de minimizar el tiempo de interrupción de las operaciones de la institución sin exponer la seguridad de las personas.

c. Criticidad: La Subgerencia Gestión de la Información determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como GRAVE.

d. Entorno: Este evento se puede dar en las instalaciones de la Subgerencia Gestión de la Información específicamente en el Data Center.

e. Personal Encargado: El Subgerente de Gestión de la Información, es quien debe dar cumplimiento a lo descrito en las condiciones de prevención de riesgo del presente plan.

f. Condiciones de Prevención de Riesgo:

Realizar inspecciones de seguridad periódicamente.

Charlas sobre el tránsito de personal autorizado o ajeno a la subgerencia.

Acatar las indicaciones de la Brigada de Emergencias del HUV.

Contar con una relación de teléfonos de emergencia que incluya el área de Seguridad y Brigada de emergencias del HUV.

Responsable de las acciones de prevención y ejecución de la contingencia.

Mantener equipos de comunicación y cámaras de vigilancia.

PLAN DE EJECUCION

a. Eventos que activan la contingencia:

La Contingencia se activará al ocurrir un ataque vandálico.

El proceso de contingencia se activará inmediatamente después de ocurrir el evento.

b. Procesos relacionados antes del evento:

Identificar la ubicación de los monitores de las cámaras de vigilancia.
Contar con una relación de teléfonos de emergencia que incluya el área de Seguridad y Brigada de emergencias del HUV.

c. Personal que autoriza la contingencia: El Subgerente Gestión de la Información o sus Representantes pueden activar la contingencia.

d. Descripción de las actividades después de activar la contingencia:
Tratar de apaciguar los ánimos del atacante o grupo de vándalos.
Comunicar al personal del área de Seguridad
Luego de calmado el suceso, se deberán realizar las siguientes actividades:
Evaluación de los daños ocasionados al personal, bienes e instalaciones.
En caso de daños del personal prestar asistencia médica inmediata
Inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
En caso de que se hayan detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.
La Coordinación Ejecutora del Plan de Contingencias deberá acordar con la Alta Gerencia del HUV., en caso de que se requiera la habilitación de espacios provisionales alternos para restablecer la función de los ambientes afectados o reubicación de los sitios de trabajo temporal.

e. Duración: La duración de la contingencia dependerá del tiempo que demande controlar el ataque.

f. DRP: este evento es de carácter interno, de alto impacto y por consiguiente debe estar incluido en el DRP.

g. Equipo de trabajo: Todo el personal de la Oficina Coordinadora de Gestion de la Información.

PLAN DE RECUPERACION

a. Personal Encargado: El personal encargado del Plan de Recuperación es la Oficina Coordinadora de Gestion de la Información, cuyo rol principal es asegurar el normal desarrollo de las operaciones del HUV.

b. Descripción: El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.

c. Mecanismos de Comprobación: El Subgerente de Gestión de la Información presentará un informe a la Gerencia Administrativa explicando que parte de las actividades u operaciones ha sido afectada y cuáles son las acciones tomadas.

d. Mecanismos de Recuperación: Se efectuara de acuerdo a las instrucciones impartidas por el personal encargado del plan:
Levantar inventario de los daños materiales y equipos de información
Adaptación del espacio provisional alterno donde se instalaran servidores, switchs y toda la infraestructura de tecnología necesaria, para conectar y habilitar toda la red de computadores del hospital.
Ante daño de equipos de cómputo, tramitar su reposición
Si hay pérdida de información: Restauración de las copias de respaldo.
e.Desactivación del Plan de Contingencia: El Subgerente Gestión de la Información o sus representantes desactivarán el plan de contingencia una vez que se hayan tomado las acciones descritas en la descripción del presente plan de recuperación, mediante una comunicación a la Coordinación Ejecutora del Plan.

f. Proceso de Actualización: El proceso de actualización será con base al informe presentado por el Subgerente de Gestión de la Información del HUV, luego de lo cual se determinaran las acciones a seguir.

PLAN DE PREVENCION EVENTO INTRUSION

a. Descripción del evento: La intrusión a los sistemas de información puede producir copia, modificación, alteración y/o borrado de datos, hasta la instalación de programas que permitan accesos no autorizados.
b. Objetivo: Establecer las normas que se ejecutaran ante un ataque informático, hacker o acceso no autorizado con el fin de minimizar el tiempo de interrupción de las operaciones de la institución.
c. Criticidad: La Subgerencia Gestión de la Información determina que el presente evento tiene un nivel de gran impacto en el servicio y se identifica como CRITICO, en cuanto a la credibilidad tanto de la subgerencia como de la misma información suministrada.
d. Entorno: Este evento se puede dar en las instalaciones de la Subgerencia Gestión de la Información específicamente en el área donde están ubicados los servidores.
e. Personal Encargado: El Subgerente de Gestión de la Información, es quien debe dar cumplimiento a lo descrito en las condiciones de prevención de riesgo del presente plan.
f. Condiciones de Prevención de Riesgo:
Realizar inspecciones de seguridad informática periódicamente.
Mantener las conexiones de redes seguras.
Instalar un sistema de firewall o cortafuegos robusto.
Crear un sistema de generación de claves periódicas seguras.
Responsable de las acciones de prevención y ejecución de la contingencia.

PLAN DE EJECUCION

a. Eventos que activan la contingencia:
La contingencia se activará al detectar una intrusión o hacker.
El proceso de contingencia se activará inmediatamente después de ocurrir el evento.
b. Procesos relacionados antes del evento:
Identificar las posibles vulnerabilidades de todo el sistema informático.
Mantener bajo máxima seguridad los sistemas de información del HUV
Tener número de teléfono del personal responsable en seguridad Informática.
c. Personal que autoriza la contingencia: El Subgerente Gestión de la Información del HUV o sus representantes pueden activar la contingencia.
d. Descripción de las actividades después de activar la contingencia:
Activar los protocolos de seguridad, cerrando todos los posibles puertos abiertos.
Hacer un escaneo a fondo de todo el sistema, para revisar la información atacada.
Realizar un inventario total de sistemas de datos, bases de datos, contraseñas, protocolos atacados, vulnerabilidades detectadas e integridad de los sistemas de seguridad.
En todo momento se coordinará con el responsable de seguridad informática, para las acciones que deban ser efectuadas por ellos.
Luego de detectado la intrusión, se deberán realizar las siguientes actividades:
Evaluación de los daños ocasionados a los sistemas de información, bienes e instalaciones informáticas.
Inventario general de la documentación, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.
En caso de que se hayan detectado bienes afectados por el evento, se evaluará el caso para determinar la reposición o restauración.
La Subgerencia Gestión de la Información del HUV deberá acordar con la Alta Gerencia del Hospital, en caso de que se requiera la habilitación de espacios provisionales alternos para restablecer la función de los ambientes afectados.
e. Duración: La duración de la contingencia dependerá del tiempo que demande controlar el ataque.
f. DRP: este evento es de carácter externo, de alto impacto y por consiguiente debe estar incluido en el DRP.
g. Equipo de trabajo: Todo el personal de la Oficina Coordinadora de Gestion de la Información.

PLAN DE RECUPERACION

a. Personal Encargado: El personal encargado del plan de recuperación es la Subgerencia Gestión de la Información del HUV, cuyo rol principal es asegurar el normal desarrollo de las operaciones del HUV., en cuanto a la información, uso de software y aplicaciones.
b. Descripción: El plan de recuperación estará orientado a recuperar en el menor tiempo posible las actividades afectadas durante la interrupción del servicio.
c.Mecanismos de Comprobación: El Subgerente de Gestión de la Información del HUV, presentará un informe a la Gerencia Administrativa explicando que parte de las actividades u operaciones ha sido afectada y cuáles son las acciones tomadas.
d. Mecanismos de Recuperación: Se efectuara de acuerdo a las instrucciones impartidas por el personal encargado del plan:
Realizar inventario de equipos y sistemas de información afectados.
Cerrar el acceso a internet a toda la red
Revisar los posibles puertos abiertos y configurar nuevamente el corta fuegos o firewall, SonicWall.
Generar y ejecutar cambios de contraseñas para todos los servidores
Permitir el acceso a la red a todos los usuarios
e. Desactivación del Plan de Contingencia: El Subgerente Gestión de la Información o sus representantes desactivarán el Plan de Contingencia una vez que se hayan tomado las acciones descritas en la descripción del presente Plan de Recuperación, mediante una comunicación a la Coordinación Ejecutora del Plan.
f. Proceso de Actualización: El proceso de actualización será con base al informe presentado por el Subgerente Gestión de la Información del HUV, luego de lo cual se determinaran las acciones a seguir.

SEGURIDAD EN LA RED DE DATOS

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 monitores 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:

- 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:
- 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.
- Firewalls: Es un sistema o combinación de sistemas, que exige normas de seguridad en la frontera entre dos o más redes.
- 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.
- 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.
- 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.
- 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.
- 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.
- 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 laspolítica 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)

Control de Seguridad de la Red:

Control 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 reglas 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.

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: 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.

Seguridad de los Equipos de Computo

Objetivo: Asegurar la protección de la información en los equipos.

Aplicabilidad: 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.

Establecimiento, uso y protección de claves de acceso.

Objetivo: Controlar el acceso a la información.

Aplicabilidad: 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” 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:

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.

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 misionales, de investigación, docente y administrativa.

Oficina coordinadora de 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 Subgerencia 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 Subgerencia 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 Subgerencia 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 Subgerencia 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 Subgerencia 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.

8. DOCUMENTOS RELACIONADOS

- Solicitud de Mantenimiento Correctivo
- Mantenimiento Preventivo de Equipos de Computo
- Solicitud de Acceso a la Web-Intranet e Internet
- Solicitud de acceso a sistemas de información
- Copia de seguridad de datos del sistema
- Copias de seguridad de datos y esquema de las bases de datos
- Copia de seguridad de archivos de transacciones Logical Logs
- Solicitud de hardware
- Solicitud de software
- Solicitud de conectividad
- Solicitud de análisis y desarrollo de software
- Publicación de información en la página Web

9. ANEXOS

N.A

10. REFERENCIAS

- Plan de Desarrollo Institucional.
- Plan de Inversión
- Presupuestos Institucional
- Plan Operativo.

- Plan de Capacitación Institucional - PIC.
- Manuales de Procedimiento
- Guías
- Protocolos
- Encuestas de Satisfacción
- Política de Calidad
- Política de Comunicaciones
- Política de Seguridad del Paciente.

Elaboró:	Revisó:	Aprobó:
Equipo de Gestión de la Información Profesional Administrativo Gestión de la Información	Soporte Calidad Soporte y Administracion Daruma Alberto Sánchez Jefe de Oficina Coordinadora de Gestión de la Información Adriana García Grosso Coordinadora de Gestión Documental	Pola Patricia Quintero Cubillos Subgerente Administrativo

Adriana García Grosso @ 2024-11-12, 16:42:22