	HOSPITAL UNIVERSITARIO DEL VALLE "EVARISTO GARCIA" E.S.E	**CÓDIGO:**	POL-HUV-HUV-003
		VERSIÓN:	001
	POLÍTICA DE SEGURIDAD DIGITAL	**FECHA DE EMISIÓN:**	2019-05-15

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 politícas, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.
Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación y su uso no autorizado.
Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.
Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.
Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.
Hardware: Refiere a todas las partes tangibles de un sistema informático; sus componentes son: eléctricos, electrónicos, electromecánicos y mecánicos. Son cables, gabinetes o cajas, periféricos de todo tipo y cualquier otro elemento físico involucrado.
Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, 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.
La presente política aquí contenida, son de observancia para la adquisición, uso de bienes y de servicios informáticos, en el HOSPITAL UNIVERSITARIO DEL VALLE “EVARISTO GARCIA” E.S.E., cuyo incumplimiento generará que se incurra en responsabilidad administrativa; sujetándose a lo dispuesto en la sección de políticas, política de cumplimiento.
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.

- 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.

6. DESARROLLO DE LA POLÍTICA

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.

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.

8. DOCUMENTOS RELACIONADOS

- PR/SSA/TIC/001 Solicitud de Mantenimiento Correctivo
- PR/SSA/TIC/002 Mantenimiento Preventivo de Equipos de Computo
- PR/SSA/TIC/003 Solicitud de Acceso a la Web-Intranet e Internet
- PR/SSA/TIC/004 Solicitud de acceso a sistemas de información
- PR/SSA/TIC/005 Copia de seguridad de datos del sistema
- PR/SSA/TIC/006 Copias de seguridad de datos y esquema de las bases de datos
- PR/SSA/TIC/007 Copia de seguridad de archivos de transacciones Logical Logs
- PR/SSA/TIC/008 Solicitud de hardware
- PR/SSA/TIC/009 Solicitud de software
- PR/SSA/TIC/010 Solicitud de conectividad
- PR/SSA/TIC/011 Solicitud de análisis y desarrollo de software
- PR/SSA/TIC/012 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	Alberto Sánchez Jefe de Oficina Coordinadora de Gestión de la Información	Pola Patricia Quintero Cubillos Subgerente Administrativo

Alberto Sánchez @ 2020-01-31, 16:44:33