

 HOSPITAL SAN VICENTE DE ARAUCA E.S.E	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACION	
	PLAN DE CONTINGENCIA	FECHA: 15/11/2022 Página: 1 de 12

PLAN DE CONTINGENCIA INFORMÁTICO

HOSPITAL SAN VICENTE DE ARAUCA ESE

2023

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030-Correo electrónico: contactenos@hospitalsanvicente.gov.co
 Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca-
 Youtube: Hospital San Vicente de Arauca, Arauca / Colombia

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACIÓN	
	PLAN DE CONTINGENCIA	FECHA: 15/11/2022 Página: 2 de 12

TABLA DE CONTENIDO

INTRODUCCIÓN.....	3
1. OBJETIVO GENERAL:.....	4
1.1. OBJETIVOS ESPECÍFICOS:.....	4
2. ALCANCE.....	4
3. RESPONSABLES.....	4
4. TERMINOS Y DEFINICIONES.....	4
5. CONDICIONES GENERALES	5
5.1 ANÁLISIS DE LA EVALUACIÓN DEL RIESGO.....	5
5.1.1 FACTORES DE AFECTAN LA SEGURIDAD FÍSICA Y LA INFRAESTRUCTURA.....	5
5.1.2 TIPOS DE RIESGOS A LOS QUE ESTÁN EXPUESTOS LOS SISTEMAS DE INFORMACIÓN EN EL HOSPITAL SAN VICENTE DE ARAUCA.....	6
5.1.3 ACTIVIDADES ASOCIADAS A LA PLANIFICACIÓN DE LA CONTINGENCIA.....	7
5.1.4 ANÁLISIS DEL RIESGO	8
5.2 IDENTIFICACIÓN DE PROCESOS CRÍTICOS O IMPACTO	9
5.3 NIVELES DE CRITICIDAD.....	9
5.4 CUANDO, CÓMO Y QUIÉN DEBE ACTIVAR EL PLAN DE CONTINGENCIA.....	10
6. CONTENIDO ESPECÍFICO	11
RELACIÓN DE LOS PROCEDIMIENTOS E INTERACCIÓN ENTRE ELLOS.....	11
7. PLAN DE ACCIÓN	12
8. ANEXOS	12
9. DISTRIBUCIÓN DEL DOCUMENTO	12

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030-Correo electrónico: contactenos@hospitalsanvicente.gov.co
Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca-
Youtube: Hospital San Vicente de Arauca, Arauca / Colombia

 HOSPITAL SAN VICENTE DE ARAUCA E.S.E	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACIÓN	
	PLAN DE CONTINGENCIA	FECHA: 15/11/2022 Página: 3 de 12

INTRODUCCIÓN

Un porcentaje muy alto de los incumplimientos en TI se debe a la caída de la infraestructura Hardware o de Software, es importante ante eventos críticos de la entidad minimizar el impacto negativo sobre la misma, los usuarios y clientes, se deben evitar interrupciones, estar preparado para fallas potenciales y guiar hacia una solución adecuada

Un plan de contingencia es un instrumento de gestión para el buen gobierno de las Tecnología de la Información y las comunicaciones en el dominio del soporte y desempeño se base en un conjunto de procedimientos alternativos a la operatividad normal de cada institución, su finalidad es la de permitir el funcionamiento de esta, aun cuando alguna de sus funciones deje de hacerlo por culpa de algún incidente tanto interno como ajeno a la institución.

Estos planes de contingencia contienen las medidas técnicas, humanas y organizativas necesarias para garantizar la continuidad de la empresa. Es un caso particular de plan de continuidad del Hospital San Vicente de Arauca busca explicar que es un plan de contingencia, el porqué de su importancia y el cómo de su preparación.

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACIÓN	
	PLAN DE CONTINGENCIA	FECHA: 15/11/2022 Página: 4 de 12

1. OBJETIVO GENERAL:

Establecer los mecanismos para afrontar de manera oportuna, adecuada y efectiva las situaciones de contingencia que puedan presentarse en los sistemas de información del Hospital San Vicente de Arauca.

1.1. OBJETIVOS ESPECÍFICOS:

1. Definir acciones y procedimientos rápidos y eficientes a ejecutar en caso de falla de uno o varios de los elementos del Sistema de información, para recobrar rápidamente el control de la información vital, ante posible pérdida o destrucción.
2. Establecer una directriz institucional que indique las acciones a seguir para garantizar el normal funcionamiento de los sistemas de información del Hospital San Vicente de Arauca.

2. ALCANCE

Este plan contempla los sistemas de información con los que cuenta el Hospital San Vicente de Arauca, busca minimizar todos los riesgos e incidentes ocasionados por fallos impredecibles.

3. RESPONSABLES

La planificación, desarrollo, verificación, control e implementación del Plan de Contingencia del Hospital San Vicente de Arauca, será responsabilidad del líder del proceso de sistemas.

4. TERMINOS Y DEFINICIONES

1. **Amenaza:** probabilidad de ocurrencia, durante un período específico y dentro de un área determinada, de un fenómeno que puede potencialmente causar daños en los elementos en riesgo.
2. **Contingencia:** Interrupción, no planificada, de la disponibilidad de recursos informáticos.

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACIÓN	
	PLAN DE CONTINGENCIA	FECHA: 15/11/2022 Página: 5 de 12

3. **Gravedad:** Se refiere a la magnitud resultante de los daños provocados por un siniestro. Esta es subdividida en ninguna, insignificante, marginal, crítica y catastrófica y se definen según el factor de evaluación (víctimas, pérdidas económicas, suspensión de operación, daño ambiental).
4. **Incidente:** Es una violación con éxito de las medidas de seguridad, como el robo de información, el borrado de archivos de datos valiosos, el robo de equipos, PC, etc.
5. **Riesgos:** es la probabilidad de que una amenaza se convierta en un desastre. La vulnerabilidad o las amenazas, por separado, no representan un peligro. Pero si se juntan, se convierten en un riesgo, o sea, en la probabilidad de que ocurra un desastre. Sin embargo, los riesgos pueden reducirse o manejarse.
6. **Plan de Contingencia:** Un plan de contingencia es el proceso de planear y documentar anticipadamente qué hacer al momento de presentarse un evento catastrófico sobre la empresa y saber identificar si por su magnitud es necesario recuperar cualquier tipo de red o el sistema informático. En resumen, es el conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y ordenada de los procesos en Red Salud Armenia E.S.E. generando un impacto mínimo al proceso de atención.
7. **Vulnerabilidad:** La vulnerabilidad se refiere al grado de pérdidas relacionadas con un elemento en riesgo (o un conjunto de elementos en riesgo), que resulta como consecuencia de un fenómeno natural o artificial con una determinada magnitud. Se expresa de una escala de “0” (no hay daños) a “1” (daño total).

5. CONDICIONES GENERALES

5.1 ANÁLISIS DE LA EVALUACIÓN DEL RIESGO

5.1.1 FACTORES DE AFECTAN LA SEGURIDAD FÍSICA Y LA INFRAESTRUCTURA

Factores ambientales

- **Incendios.** Los problemas derivados del entorno eléctrico que suministra los equipos pueden presentar cortocircuitos.
- **Inundaciones.** Es la invasión de agua por exceso de escurrimientos superficiales o por acumulación en terrenos planos, ocasionada por falta de

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030-Correo electrónico: contactenos@hospitalsanvicente.gov.co

Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca-

Youtube: Hospital San Vicente de Arauca, Arauca / Colombia

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACIÓN	
	PLAN DE CONTINGENCIA	FECHA: 15/11/2022 Página: 6 de 12

drenaje ya sea natural o artificial. Esta es una de las causas de mayores desastres en centros de cómputo.

- **Sismos.** Son temblores o vibraciones, que causan la caída de soportes informáticos físicos, o la destrucción de las infraestructuras que permiten su correcto funcionamiento, es una amenaza significativa.
- **Humedad.** En ambientes extremadamente secos el nivel de electricidad estática es elevado, lo cual puede llegar a transformar un pequeño contacto entre persona y circuito, o entre diferentes componentes, en un daño irreparable al hardware y, por ende, a la información que contiene. Sin embargo, altos niveles de humedad son perjudiciales para los equipos, pudiendo llegar a producir condensación en los circuitos integrados, originando cortocircuitos.

Factores humanos

- **Robos.** Los computadores son posesiones valiosas de las empresas y están expuestas a que sean sustraídos de las instalaciones del Hospital San Vicente de Arauca, al igual que la información que reposa en cada uno de ellos.
- **Actos vandálicos.** Se puede dar por empleados descontentos que pueden tomar represalias contra los equipos y las instalaciones o por factores externos.
- **Fraude.** Cada año millones de pesos son sustraídos de las empresas, uno de los medios es a través de los computadores de las instituciones.
- **Sabotaje.** Es el peligro más temido en los centros de cómputo. Empresas que han intentado implementar sistemas de seguridad de alto nivel, han encontrado que la protección contra el saboteador es uno de los retos más duros, el saboteador puede ser un empleado o un sujeto ajeno a la empresa.
- **Terrorismo.** Son actos causados por la violencia que se presenta en el territorio y que pueden ir dirigidos a perjudicar al Hospital San Vicente de Arauca.

5.1.2 TIPOS DE RIESGOS A LOS QUE ESTÁN EXPUESTOS LOS SISTEMAS DE INFORMACIÓN EN EL HOSPITAL SAN VICENTE DE ARAUCA.

- Falla en los equipos
- Falla de los aplicativos
- Acción de un virus informático
- Fenómenos Naturales
- Accesos no autorizados
- Pérdida de datos

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030-Correo electrónico: contactenos@hospitalsanvicente.gov.co
 Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca-
 Youtube: Hospital San Vicente de Arauca, Arauca / Colombia

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACIÓN	
	PLAN DE CONTINGENCIA	FECHA: 15/11/2022 Página: 7 de 12

- Incendio o fuego
- Robo de equipos y archivos
- Manipulación o sabotaje

5.1.3 ACTIVIDADES ASOCIADAS A LA PLANIFICACIÓN DE LA CONTINGENCIA

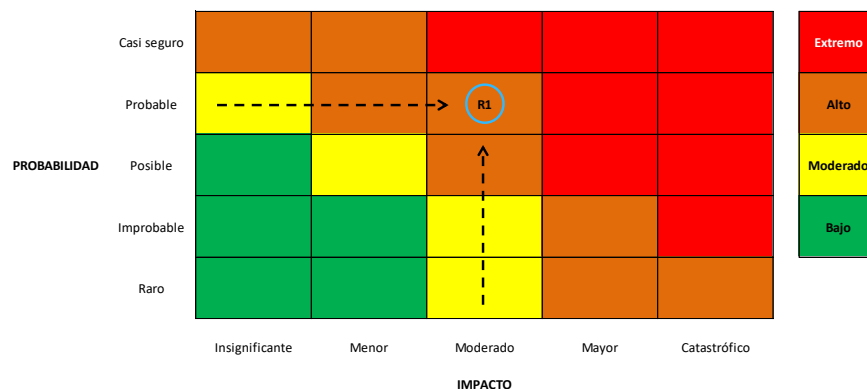
1. **Análisis de riesgos:** se procede a identificar los objetos que deben ser protegidos, los daños que pueden sufrir, sus posibles fuentes de daño y oportunidad, su impacto en el hospital y su importancia dentro del funcionamiento del Hospital San Vicente de Arauca
2. **Identificación de procesos críticos o impacto:** se clasifica en prioridades de acuerdo con el impacto que causas
 - a. **Prioridad alta:** corresponde a todas aquellas herramientas, que en caso de no ser restauradas oportunamente generarían graves problemas en la prestación del servicio a los usuarios
 - b. **Prioridad media:** corresponde a todas aquellas herramientas, que, aunque son importantes para el desarrollo normal de las actividades administrativas, operativas y de control, no son críticas para la prestación del servicio a los usuarios del Hospital San Vicente de Arauca.
 - c. **Prioridad baja:** Son sistema cuya falla causa molestias menores, corresponde a todas aquellas herramientas cuya falla no representa graves traumatismos en la prestación del servicio a los usuarios y su puesta en funcionamiento puede tardar en restaurar el sistema sin ningún problema para el Hospital San Vicente de Arauca.
3. **Niveles de criticidad**
4. **Cuando, cómo y quién debe activar el Plan de contingencia.**

	SISTEMA INTEGRADO DE GESTIÓN		CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL		VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACION		FECHA: 15/11/2022
	PLAN DE CONTINGENCIA		Página: 8 de 12

5.1.4 ANÁLISIS DEL RIESGO

No.	Descripción del riesgo	Causas	Consecuencias	Probabilidad	Impacto	Riesgo Inherente	Acciones preventivas o de mejora
R1	Pérdida de información de las bases de datos del sistema de información institucional Dinámica	Falla total del servidor Principal de la Base de Datos del Hospital San Vicente de Arauca	1. Pérdida de información de las bases de datos del Sistema de Información 2. Problemas para reiniciar labores con normalidad en el Sistema de Información	Posible	Moderado	Medio	1. Garantizar que las copias de seguridad del servidor se realicen según lo establecido.
R2	Pérdida de información de los equipos de cómputo	1. Incursión de Malware 2. Software maliciosos 3. Virus informáticos	1. Pérdida de información administrativa, financiera y asistencial 2. Problemas para realizar labores con normalidad en los sistemas de información	Posible	Moderado	Medio	1. Copias de seguridad de los equipo de cómputo 2. Anti Virus actualizado en cada equipo de cómputo 3. Cumplimiento del plan anual de mantenimiento
R3	Falla general en la red de datos	1. Fallas en switches o routers 2. Descargas de videos de alta definición 3. Caídas del servicio de internet	1. Inconvenientes para la atención de usuarios 2. Problemas para realizar labores con normalidad en los sistemas de información	Posible	Moderado	Medio	Realizar seguimiento Diario al estado de la red de datos
R4	Manipulación de los datos e información de los equipos de cómputo	1. Vulneración, adulteración o uso indebido de la información. 2. Desconocimiento de las políticas de seguridad y privacidad de la información	1. Pérdidas económicas 2. Sanciones legales	Improbable	Moderado	Moderado	1. Divulgar las políticas de seguridad y privacidad de la información 2. Anti Virus actualizado en cada equipo de cómputo
R5	Daño en equipos de computo	1. Incumplimiento del plan de mantenimiento 2. Cableado en mal estado 3. Problemas de humedad 4. Temperatura inapropiada 5. Falta de presupuesto para compra de equipos 6. Falta de presupuesto para compra de partes dañadas	Daños en equipos, fallas en las aplicaciones y pérdida en la continuidad de la prestación del servicios	Casi seguro	Mayor	Extremo	1. Respaldo con ups a equipos sensibles de la plataforma tecnológica. 2. Revisión de las condiciones de humedad y temperatura de los ambientes 3. Disponibilidad de equipos de respaldo para ser suministrados
R6	Indisponibilidad del sistema	1. Daño por hardware en el servidor. 2. Caída por fluido eléctrico. 3. Daños en el sistema de información por código malicioso 4. Fallas en la red de datos. 5. Control de acceso al sistema operativo. 6. Posibles fallas en el fluido eléctrico	1. Pérdida de la información 2. Modificación de la información 3. Inoportunidad de la atención. 4. Reproceso	Posible	Mayor	Extremo	1. Ups 2. Recurso humano disponible 3. Antivirus 4. Realizar pruebas al plan de contingencia

Mapa de Riesgo



“Trabajando por la Salud del pueblo Araucano”

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACIÓN	
	PLAN DE CONTINGENCIA	FECHA: 15/11/2022 Página: 9 de 12

5.2 IDENTIFICACIÓN DE PROCESOS CRÍTICOS O IMPACTO

El presente Plan de contingencia se considera requerido en todos los sistemas de prioridad Alta, recomendable para todos los sistemas de prioridad media y sugerido para todos los sistemas de prioridad baja.

- **PRIORIDAD ALTA**
 - Módulos administrativos y asistenciales del aplicativo Dinámica Gerencial Hospitalaria
 - Directorio Activo
 - Servidor de Bases de datos
 - Sistema operativo de servidores
 - Backus de la información
- **PRIORIDAD MEDIA**
 - Servicio de internet
 - Correo electrónico
 - Antivirus
- **PRIORIDAD BAJA**
 - Herramientas de Microsoft Office

5.3 NIVELES DE CRITICIDAD

Luego que se realice por parte del área de Sistemas el diagnóstico de la eventualidad presentada, se catalogará en los siguientes niveles de criticidad:

- **ALTA**

Cuando el criterio del profesional de salud sobre la interrupción del Sistema de información exige la activación de un mecanismo interno para poder continuar con la atención de un paciente
- **MEDIA**

Cuando la interrupción del Sistema de información dura más de 1 hora, pero se requiere activar un mecanismo alterno para poder concluir oportunamente la atención del paciente. Es una situación prioritaria pero no urgente (Ejemplo: solicitud de exámenes prioritarios, prescripción de medicamentos, anotaciones en la historia clínica, consulta externa, facturación, etc.)

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACIÓN	
	PLAN DE CONTINGENCIA	FECHA: 15/11/2022 Página: 10 de 12

- **BAJA**

Cuando la interrupción del Sistema de información dura más de 1 hora, pero los procesos pueden esperar hasta 24 horas sin afectar la atención del paciente y permite espera el restablecimiento del Sistema de información a la normalidad (Ejemplo: respuestas a glosas, informes financieros, etc.)

5.4 CUANDO, CÓMO Y QUIÉN DEBE ACTIVAR EL PLAN DE CONTINGENCIA

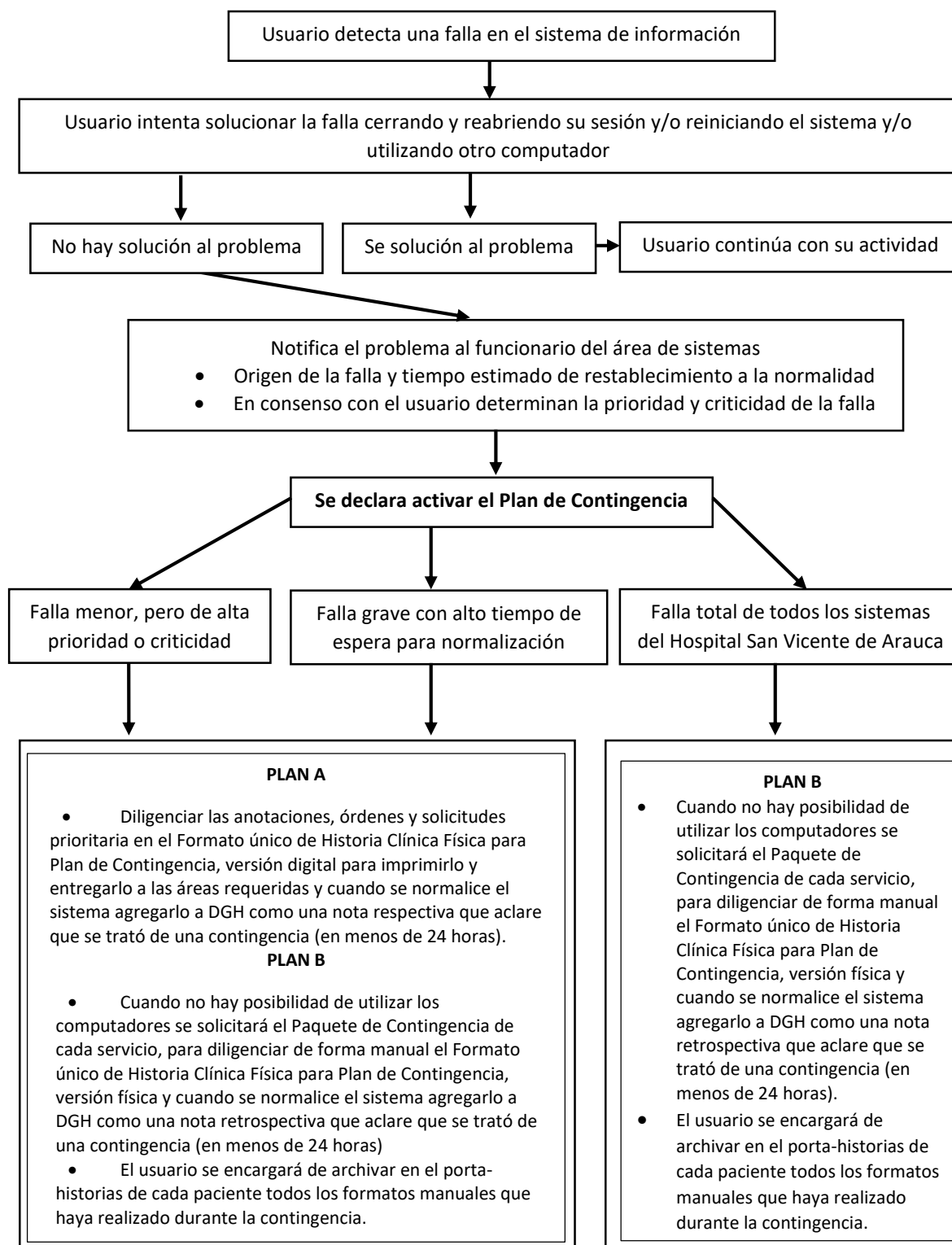
El proceso para la activación de los planes de contingencia es el siguiente:

- El usuario informará al área de sistemas sobre la falla presentada
- El personal de sistema realizará la revisión del fallo informado, verificando si es una falla leve y no cumple con los parámetros de prioridad y criticidad y no amerita la activación del Plan de Contingencia. En caso de que la falla cumpla con los parámetros de prioridad y criticidad en evaluación conjunta con el usuario, se activará el del Plan de Contingencia desde ese momento.
- El personal de Sistemas deberá catalogar el inconveniente en los parámetros de prioridad y criticidad e informará a las áreas afectadas, así como el tiempo estimado para la solución del inconveniente.
- Luego de haber solucionado el inconveniente el área de sistemas informará a las áreas que el inconveniente ha sido solucionado y se cerrará el plan de contingencia, de lo cual dejará constancia en un acta específica de la contingencia ocurrida
- Los formatos manuales realizados durante la contingencia son responsabilidad de cada área y estos deben ser reportados a las áreas que les correspondan.

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACIÓN	FECHA: 15/11/2022
	PLAN DE CONTINGENCIA	Página: 11 de 12

6. CONTENIDO ESPECÍFICO

RELACIÓN DE LOS PROCEDIMIENTOS E INTERACCIÓN ENTRE ELLOS



"Trabajando por la Salud del pueblo Araucano"

	SISTEMA INTEGRADO DE GESTIÓN	CODIGO: GTD-SI-PL-004
	PROCESO: GESTIÓN TECNOLÓGICA Y DOCUMENTAL	VERSIÓN: 01
	SUBPROCESO: SISTEMAS DE INFORMACIÓN	FECHA: 15/11/2022
	PLAN DE CONTINGENCIA	Página: 12 de 12

7. PLAN DE ACCIÓN

Formato en excell debidamente diligenciado

8. ANEXOS

GDE-GC-FR-021 Formato plan de acción

9. DISTRIBUCIÓN DEL DOCUMENTO

Este documento debe reposar en intercambio Aragón, en el proceso de sistemas

CONTROL DE DOCUMENTO				
VERSION	FECHA APROBACIÓN			MOTIVO
	DIA	MES	AÑO	
01	16	11	2022	Creación del documento

ELABORÓ/ACTUALIZO FIRMA:	REVISÓ FIRMA:	VIABILIZÓ: FIRMA:	APROBO: FIRMA:
Freddy Cabrera	Ana Isabel Cely Abril Sara Eddy Maldonado	Claudia Genara Pérez	Comité institucional de gestión y desempeño
Líder del proceso de Sistemas.	Profesional de apoyo del proceso Gestión y Garantía de la calidad Líder del proceso de Gestión y Garantía de la Calidad	Subdirección Administrativa	CARGO: Acta de Comité No. 006 del 2022
15/11/2022	15/11/2022	15/11/2022	16 Noviembre del 2022

“Trabajando por la Salud del pueblo Araucano”

Calle 15 16-17 Esquina. PBX (097) – 8850030-Correo electrónico: contactenos@hospitalsanvicente.gov.co
Página Web: www.Hospitalsanvicente.gov.co- Facebook Hospital San Vicente Arauca- Twitter: @SanArauca-
Youtube: Hospital San Vicente de Arauca, Arauca / Colombia