

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
		FECHA: 21/07/2025
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	TRD: PÁGINA: 1 de 15

PLAN DE CONTINUIDAD DEL NEGOCIO, PLAN DE CONTINGENCIA

CONTROL DE CAMBIOS DE DOCUMENTO

VERSION	ORIGEN DE LOS CAMBIOS	FECHA DE REGISTRO			CARGO DEL FUNCIONARIO
		DIA	MES	AÑO	
1	Creación del documento	08	01	2021	Ingeniera de sistemas
2	Actualización	27	06	2024	Ingeniera de sistemas
3	Actualización	21	07	2025	Ingeniera de sistemas

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
		FECHA: 21/07/2025
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	TRD: PÁGINA: 2 de 15

INTRODUCCIÓN

La implementación de un proceso de preservación de la información pública ante situaciones disruptivas, permite minimizar el impacto y recuperación por pérdida de activos de información del **HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**, hasta un nivel aceptable mediante la combinación de controles preventivos y de recuperación.

En este proceso, es fundamental identificar los procesos críticos para el negocio. Asimismo, es conveniente integrar los requisitos de la gestión de la seguridad de la información y la continuidad del negocio con otras necesidades de continuidad. Esto incluye aspectos relacionados con operaciones, personal, materiales, transporte e instalaciones.

Las consecuencias de eventos disruptivos (desastres, fallas de seguridad, pérdida del servicio y disponibilidad del servicio) se deberían someter a un análisis del impacto del negocio (BIA). Se deben desarrollar e implementar un plan de continuidad que permita garantizar la restauración oportuna de las operaciones esenciales.

Una correcta implementación de la gestión de la continuidad del negocio disminuye la posibilidad de que ocurran incidentes disruptivos. En caso de que estos se presenten, la organización estará preparada para responder de manera adecuada y oportuna, lo que reducirá significativamente el daño potencial.

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
		FECHA: 21/07/2025
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	TRD: PÁGINA: 3 de 15

JUSTIFICACIÓN

La gestión de la continuidad del negocio es un proceso holístico esencial que permite al HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. identificar y mitigar los impactos potenciales que amenazan sus operaciones. Este enfoque integral provee el marco necesario para construir resiliencia y una capacidad de respuesta efectiva, asegurando así la protección de los intereses de la entidad frente a cualquier interrupción.

GLOSARIO

❖ Sitio alterno.

Ubicación alterna de operaciones seleccionada para ser utilizada por una organización cuando las operaciones normales no pueden llevarse a cabo utilizando las instalaciones normales después de que se ha producido una interrupción.

❖ Gestión de continuidad de negocio (BCM).

Proceso general de gestión holístico que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio que en caso de materializarse y el cual provee un marco de trabajo para la construcción de la resiliencia organizacional con la capacidad de una respuesta efectiva que salvaguarde los intereses de las partes interesadas claves, reputación, marca y actividades de creación de valor.

❖ Plan de Continuidad de Negocio.

Procedimientos documentados que guían orientan a las organizaciones para responder, recuperar, reanudar y restaurar la operación a un nivel predefinido por la operación debido una vez presentada / tras la interrupción.

NOTA: Típicamente, esto incluye los recursos, servicios y actividades necesarios para garantizar la continuidad de las funciones críticas del negocio. [Fuente: ISO 22301]

❖ Análisis del impacto al negocio (BIA por sus siglas en ingles).

Proceso del análisis de actividades las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. [Fuente: ISO 22300]

❖ Nivel de Criticidad.

Descripción cualitativa usada para enfatizar la importancia de un recurso, proceso o función que debe estar disponible y operativa constantemente o disponible y operativa al menor tiempo posible después de que un incidente, emergencia o desastre ocurra.

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	FECHA: 21/07/2025
		TRD:
		PÁGINA: 4 de 15

❖ **Interrupción.**

Incidente, bien sea anticipado (ej. huracanes) o no anticipados (ej. Fallas de potencia, terremotos, o ataques a la infraestructura o sistemas de tecnología y telecomunicaciones) los cuales pueden afectar el normal curso de las operaciones en alguna de las ubicaciones de la organización.

❖ **Recuperación de desastres de tecnología y telecomunicaciones (ITCTIC).**

Habilidad Capacidad de los elementos de tecnología y telecomunicaciones (ITC) de las TIC de la organización para soportar sus funciones críticas a un nivel aceptable dentro de un periodo predeterminado de tiempo después de una interrupción.

❖ **Plan de recuperación de desastres de ICT LAS TIC (ICT DRP).**

Plan claramente definido y documentado el cual permite recuperar las capacidades de tecnología y Telecomunicaciones LAS TIC cuando se presenta una interrupción.

NOTA: En algunas organizaciones es llamado el plan de continuidad de tecnología y telecomunicaciones las TIC.

❖ **Modo de falla.**

Manera Forma en por la cual se observa una falla es observada.

NOTA: Esta generalmente describe la manera en que la falla ocurre y su impacto para en la operación del sistema.

❖ **Preparación de las ICT TIC para la continuidad de negocio (IRBC).**

Capacidad de una organización para soportar sus operaciones de negocio mediante la prevención, detección y respuesta a una interrupción, así como la recuperación de sus servicios de ICTTIC.

❖ **Objetivo mínimo de continuidad de negocio (MBCO).**

Mínimo nivel de productos y/o servicios que es aceptable para que la organización alcance sus objetivos de negocio durante una interrupción.

❖ **Punto objetivo de recuperación (RPO).**

Punto en el tiempo en el cual los datos deben ser recuperados después de que una interrupción ocurra.

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
		FECHA: 21/07/2025
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	TRD: PÁGINA: 5 de 15

❖ **Punto Tiempo objetivo de tiempo de recuperación (RTO).**

Periodo de tiempo en el cual los mínimos niveles de productos y/o servicios y los sistemas, aplicaciones, o funciones que los soportan deben ser recuperados después de que una interrupción ocurra.

❖ **Resiliencia.**

Habilidad Capacidad para que una organización para resistir cuando es afectada al ser afectada por una interrupción.

❖ **Disparador o detonante.**

Evento que hace que el sistema inicie una respuesta.

NOTA: También conocido como evento activador.

❖ **Registro vital.**

Registro electrónico o en papel que es esencial para preservar, continuar o reconstruir las operaciones de una organización y proteger los derechos de una organización, sus empleados.

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	FECHA: 21/07/2025
		TRD:
		PÁGINA: 6 de 15

OBJETIVOS

Para lograr esta visión, se han adoptado los siguientes objetivos para el **HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E:**

- ❖ Establecer procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones críticas del negocio que se puedan ver comprometidas por eventos naturales, o sean ocasionados por el hombre.
- ❖ Identificar las aplicaciones y las plataformas consideradas críticas para la operación del negocio.
- ❖ Establecer los tiempos mínimos de recuperación requeridos en los que no se vea afectado el negocio.
- ❖ Definir la funcionalidad mínima que requiere el negocio en caso de contingencia.
- ❖ Identificar los riesgos presentes para la continuidad.
- ❖ Establecer los elementos esenciales requeridos en el plan de recuperación de desastres.
- ❖ Desarrollar procedimientos específicos y guías de operación en caso de desastre para cada uno de los servicios críticos vitales especificados en el alcance del plan.
- ❖ Desarrollar e impartir la capacitación inicial para el correcto funcionamiento del plan.
- ❖ Establecer un plan de prueba, gestión y mantenimiento necesarias para garantizar los objetivos del Plan.

PLANES DE CONTINUIDAD Y CONTINGENCIAS DEL NEGOCIO

Gestión de continuidad de negocio

Planes de recuperación:

CAIDA DEL SISTEMA APLICATIVO: En caso de una interrupción del sistema de información, se activará el siguiente procedimiento para garantizar la continuidad operativa:

- ❖ **Comunicación Interna:** El área de sistemas informará inmediatamente sobre la caída del sistema a través de los canales de comunicación interna establecidos.
- ❖ **Modo Manual - Área Asistencial:** El personal asistencial operará de forma manual. Se solicitará al almacén, o en su defecto a la subgerencia científica, la papelería física necesaria para el registro de historias clínicas, ordenaciones y prescripciones. Esto se mantendrá hasta que el sistema se restablezca.
- ❖ **Modo Manual - Facturación:** El equipo de facturación verificará y gestionará la información utilizando las bases de datos de respaldo en Excel disponibles.

Este procedimiento asegura que tanto la atención asistencial como la facturación puedan continuar con sus actividades esenciales durante la interrupción del sistema principal.

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	FECHA: 21/07/2025
		TRD:
		PÁGINA: 7 de 15

Cuando se presenta una falla en el acceso al aplicativo o se deniega el mismo, contactamos a las líneas de soporte y mesa de ayuda de SINERGIA S.A., la empresa desarrolladora del software. Ellos, a través de su servicio 7x24 para servidores en caso de caídas, resuelven el inconveniente restableciendo el acceso.

CAIDA DE LA ENERGIA: los equipos con **UPS** (Sistema de Alimentación Ininterrumpida) mantienen la carga eléctrica por hasta 10 minutos, tiempo suficiente para un apagado normal. Si el corte excede los 10 minutos, una **planta eléctrica automática** a nivel hospitalario se activa dentro de los 10 primeros segundos, suministrando energía a los equipos de cómputo y permitiendo continuar el trabajo hasta que se restablezca el servicio eléctrico regular.

CAIDA DE LA RED DE DATOS: Cuando la **red de datos** sufre una caída, tanto en el hospital como en sus sedes, se activa el **plan de contingencia manual** y se comunica la situación por los medios internos. Una vez restablecido el servicio, se informa de la misma manera.

Cuando vuelve el sistema a funcionar, en estadística se lleva la papelería y luego es cargada al sistema de información por el personal asistencial.

CAIDAS DEL INTERNET: Se tiene 2 proveedores de internet, ERT y SERVINET los cuales están subdivididos según el trabajo que realizan los usuarios, la ERT tiene 200 megas dedicada de velocidad, y SERVINET 600 megas cuando se cae el internet a nivel masivo se restablece o se cambia al que no esté dañado por medio de una **VPN (Virtual Private Network)**, o **Red Privada Virtual**, La cual realiza este proceso automáticamente.

Para la Facturación electrónica se cuenta con un internet independiente de 200 megas de velocidad de la ERT y un correo electrónico de Google facturacion@sanrafaelzarzal.gov.co por el cual se envían las facturas electrónicas a la DIAN y está disponible para esta labor.

El área de Tesorería también cuenta con un Internet independiente de 50 megas de velocidad de la ERT.

DAÑOS EN HARDWARE: Cuando hay daños se tienen equipos de respaldos los cuales según la necesidad, se prioriza las áreas de servicio asistenciales las cuales atienden los pacientes y se colocan respaldos mientras se da solución a los equipos e impresoras, se tiene portátil o torres, monitores, y remanentes en el almacén y en sistemas de mouse y teclados, sino se tienen también a la mano o se usa un proveedor externo que nos provee y nos cubre las necesidades de los equipos e impresoras (Grupo ITC).

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	FECHA: 21/07/2025
		TRD:
		PÁGINA: 8 de 15

EVALUACIÓN DE IMPACTOS OPERACIONALES

La tabla siguiente muestra los niveles de criticidad del Hospital, que contempla un sistema de tolerancia a fallas por horas, cuya propiedad permite que un sistema pueda seguir operando normalmente a pesar de que una falla haya ocurrido en alguno de los componentes del sistema; por lo tanto, la tolerancia a fallas es muy importante en aquellos sistemas que deben funcionar todo el tiempo.

Categoría (Función del Negocio)	Proceso (Servicios)	Nivel	Tolerancia a Fallas (Horas)	Descripción
Aplicaciones	Sistema de Control de flujo de documentos	B	3	Contenedor de aplicaciones
Web	Sitio web Entidad	A	1	Capa de presentación
Base de Datos	Sistema de información aplicativo	A	1	Contenedor de aplicaciones en SQL
Seguridad	Dispositivos de redes	A	1	Servicio de firewall de la Entidad
Sistemas de almacenamiento	SAN (Storage Area Network)	A	3	Capacidad de almacenamiento en SAN
Comunicaciones	Acceso Local a Internet	C	4	Comunicación de Internet del usuario local
Cuartos de cableado	Centro de cableado y gabinetes central	A	1	Servicio de Centro de datos de la Entidad
Proveedores Aplicaciones	Interno/externo	B	2	Desarrollo Interno o contratado Por externos. Canales de comunicaciones
Recurso Humano	Internos/externos	C	3	Profesionales encargados de administrar las infraestructuras de la Entidad

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	FECHA: 21/07/2025
		TRD:
		PÁGINA: 9 de 15

IDENTIFICACIÓN DE PROCESOS CRÍTICOS

La identificación de los procesos críticos del negocio se da con base en la clasificación de los impactos operacionales de las organizaciones, según esta tabla.

Valor	Interpretación del proceso crítico
A	Crítico para el Negocio, la función del negocio no puede realizarse
B	No es crítico para el negocio, pero la operación es una parte integral del mismo.
C	La operación no es parte integral del negocio.

IDENTIFICACIÓN DE RECURSOS

Las diferentes actividades contempladas en la función crítica del negocio deben considerarse de vital importancia cuando apoyan los procesos críticos del negocio; por lo tanto, es clave en este punto, la identificación de recursos críticos de Sistemas de Tecnología de Información que permitan tomar acciones para medir el impacto del negocio de las Entidades.

La siguiente tabla representa un ejemplo de identificación de recursos críticos de sistemas de Tecnologías de Información.

Categoría (Función Crítica del Negocio)	Procesos Críticos (Servicios)	Identificación de recursos críticos de Sistemas TI
Aplicaciones	- Sistema de información Sihos - Interfaz de laboratorio AnnarLab - Página Institucional	- Sistema de información asistencial y financiero. - Sistema de información asistencial para laboratorio. - Información interna y externa de la entidad.
Seguridad de Información	Protección con contraseñas	Reglas de entrada y acceso al sistema
Comunicaciones	Servicio Wifi	Control de usuarios locales Vs Invitados.
Centro de cableado central o gabinetes, servidores	Centro de datos	Control de operaciones de Servidores, Equipos de Comunicaciones, Sistemas de Almacenamiento, Sistemas de Backups, Aire Acondicionado, Acometida Eléctrica.

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	FECHA: 21/07/2025
		TRD: PÁGINA: 10 de 15

La siguiente tabla muestra un ejemplo de valores RTO/WRT para el proceso crítico de la operación del Centro de Datos de una organización.

Categoría (Función Crítica del Negocio)	Procesos Críticos (Servicios)	Identificación de recursos críticos de Sistemas TI	Tiempo de Recuperación Objetivo – RTO	Tiempo de Recuperación de Trabajo – WRT
Centro de cableado central ogabinetes, servidores	Centro de Datos	Control de operaciones de Servidores. Sistemas de Almacenamiento. Sistemas de Backups (Discos y nube). Aire Acondicionado, Acometida Eléctrica	1 día 0.5 día 1.5 días 2 días	1 día 0.5 día 1.5 días 2 días

Esta imagen representa el diseño de la infraestructura de respaldo de la entidad. Se destaca la implementación de un servidor réplica central para la salvaguarda continua de la información crítica. La estrategia incluye la generación de copias de seguridad manual en discos duros locales (para recuperación rápida) y una copia adicional manual en la nube (para recuperación ante desastres y redundancia geográfica), garantizando así la disponibilidad de los datos y la resiliencia de las operaciones frente a interrupciones. Las copias de seguridad, se realizan a la Base de Datos del Hospital, el Proyecto del sistema de información nombrado en el contrato y, a las imágenes y archivos.

backups

Nombre	Fecha de modificación	Tipo	Tamaño
proyecto-2025-07-30_13-10-01.tar.gz	30/07/2025 1:18 p. m.	Archivo GZ	11.085.694 KB
backupHSRZ_20250730120001.sql.gz	30/07/2025 12:21 p. m.	Archivo GZ	8.012.196 KB
backupHSRZ_20250730050001.sql.gz	30/07/2025 5:21 a. m.	Archivo GZ	8.266.787 KB
disk2-2025-07-30_02-00-01.tar.gz	30/07/2025 3:08 a. m.	Archivo GZ	92.410.217 KB
backupHSRZ_20250729190001.sql.gz	29/07/2025 7:20 p. m.	Archivo GZ	7.982.915 KB

GESTIÓN DEL RIESGO:

Riesgos Tecnológicos:

- ❖ Fallas en el Fluido Eléctrico.
- ❖ Sabotaje Informático.
- ❖ Fallas en el Centro de Datos
- ❖ Problemas Técnicos.
- ❖ Fallas en equipos tanto de procesamiento, telecomunicaciones como eléctricos.
- ❖ Servicios de Soporte a Sistemas de Producción y/o Servicios.

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
		FECHA: 21/07/2025
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	TRD: PÁGINA: 11 de 15

Riesgos Humanos:

- ❖ Acto Hostil.
- ❖ Marchas, mítines.
- ❖ Artefactos explosivos.
- ❖ Problemas organizacionales (huelgas, leyes aceptadas por el congreso, regulaciones gubernamentales, leyes internacionales)
- ❖ Problemas de terceros involucrados en la producción o soporte a un servicio.
- ❖ Problemas con los proveedores de insumos o subproductos.

Desastres Naturales:

- ❖ Sismos
- ❖ Tormentas Eléctricas
- ❖ Incendios
- ❖ Inundaciones

CLASIFICACIÓN DE ESCENARIOS DE RIESGO

A fin de conocer con precisión, los riesgos potenciales de la prestación de servicios de tecnologías de la información en las Entidades, es recomendable clasificar los posibles escenarios de los riesgos potenciales y describir su nivel de impacto por cada función crítica del negocio. La siguiente tabla describe un ejemplo de esta clasificación.

Categorías	Escenarios	Descripción Impacto
Red Eléctrica	Fallas en el fluido eléctrico red normal (no regulada)	Fallas del servicio eléctrico de la entidad que afecta equipos eléctricos normales.
	Fallas en el Fluido Eléctrico red regulada	Fallas en los servicios de Tecnología de Información.
Red Datos, Internet y Seguridad	Problemas dispositivos Red: Falla Parcial	Falla temporal de los servicios de TI de todo un componente por limitación en la comunicación.
	Problemas dispositivos Red: Falla Total	Falla general de los servicios de TI de todos los componentes por ausencia en las comunicaciones
	Problemas en los Dispositivos Seguridad: Falla Parcial	Falla parcial de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware Software) y ausencia de políticas y controles de TI.
	Problemas en los Dispositivos Seguridad: Falla Total	Falla general de los servicios de TI de todos los componentes que tiene que ver con elementos de seguridad de TI (Elementos de Hardware, Software) y ausencia de políticas y controles de TI.

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	FECHA: 21/07/2025
		TRD: PÁGINA: 12 de 15

	Ausencia servicio del canal de Internet Última Milla: Total	Falla general de los servicios de TI de todos los componentes involucrados en la conexión de última milla por ausencia en la comunicación. No acceso a internet; impacto directo con el proveedor del servicio.
	Perdida conectividad Parcial	Falla parcial de los servicios de TI por ausencia en la conexión hacia. Acceso parcial a la red de internet por parte del proveedor del servicio.
Hardware distribuido	Problema de Hardware de Servidores: Falla Total	Falla total de los servicios de los sistemas de información que usan la plataforma de servidores.
	Problema Hardware Servidores: Falla Parcial	Degradación de la calidad (lentitud) de los servicios de los sistemas de información que usan la plataforma de servidores.
	Problemas en sistema Almacenamiento	Falla de los servicios de los sistemas de Información que usan la plataforma de almacenamiento de información.
	Problemas Hardware de Servidores	Falla de los servicios de los sistemas de información que usan la plataforma de servidores.
Aplicaciones infraestructura distribuida	Problemas Capa de Aplicaciones	Falla o degradación del servicio prestado en el sistema de información afectado por problemas en las aplicaciones.
	Problemas Capa Media	Falla o degradación de la aplicación soportada por las herramientas de software y el sistema de almacenamiento masivo de datos – SAN, por tanto se puede presentar degradación o ausencia del servicio prestado por sistema de información afectado por problemas de la capa media.
	Problemas de Bases de Datos	Falla o degradación de las aplicaciones soportadas por las herramientas y motores de Base de Datos, por tanto se puede presentar degradación o ausencia del servicio prestado por los sistemas de información afectados por problemas de la capa de base de datos.
Recurso Humano	Ausencia de funcionarios, incapacidades y rotación	Disminución de capacidad de atención a los clientes y usuarios, lentitud en la atención a requerimientos e incidentes, como también el retraso en la puesta en marcha de nuevos servicios.
	Errores humanos en operación	Contempla desde la degradación de un servicio hasta la pérdida del mismo, como también la ejecución de procedimientos de manera errada que dé como resultado la pérdida del servicio de uno o todos los sistemas de información del proyecto.

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
		FECHA: 21/07/2025
		TRD:
		PÁGINA: 13 de 15

Desarrollo de aplicaciones	Falla en la aplicación por desarrollo no adecuado de parte de terceros	Contempla la degradación de un servicio por fallas en la funcionalidad de los sistemas de información.
	Falla en la aplicación por desarrollo no adecuado por parte de la Entidad	Contempla la degradación de un servicio por fallas en la funcionalidad en los sistemas de información de la Entidad.

IDENTIFICACIÓN DE VULNERABILIDADES

Estas no son causa necesariamente de daño, sino que son condiciones que pueden hacer que una amenaza afecte a un activo de información en particular. Para cada amenaza identificada en el punto anterior se debe realizar un análisis de riesgo para identificar la(s) vulnerabilidad(es).

La siguiente tabla muestra un ejemplo de las amenazas y vulnerabilidades por cada Activo de Información.

Sistema TI	Activo de Información	Amenaza	Vulnerabilidad	Probabilidad de ocurrencia	Impacto
Servicio Web de la Entidad	Página Web Entidad	(desfiguración página web)	Mal diseño del sitio web	Medio	Alto
Servicio de correo electrónico	Correo electrónico Exchange	Virus, listas negras	Carencia de parches de seguridad	Alto	Alto
Sistema de Almacenamiento	SAN o NAS	Falla en el fluido eléctrico	No hay buena acometida eléctrica	Bajo	Alto
Sistema de Base de datos	Bases de datos interna	Usuario no autorizado	Mala configuración	Bajo	Alto
Servicio Red de comunicaciones	Equipos Switches de la Entidad	Falla de comunicaciones	Bloqueo de puertos	Medio	Alto

	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
		FECHA: 21/07/2025
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	TRD: PÁGINA: 14 de 15

CONCLUSIONES

Se finaliza con el análisis de impacto del negocio, que hace parte importante del plan de continuidad del negocio y a su vez presenta consideraciones importantes para la gestión del riesgo dentro del **HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E.**, que establecen un marco de políticas, procedimientos y estrategias que permiten asegurar que las operaciones de carácter crítico puedan ser mantenidas y recuperadas a la mayor brevedad posible, en caso de fallas graves dentro de los sistemas de información y las comunicaciones.

Se concluye que, la organización debe considerar que el instrumento operacional es muy importante que permite la toma de decisiones en momentos críticos de la organización en virtud del cese de operaciones debido a una situación anómala presentada. De esta manera dicho instrumento, contribuye a identificar las operaciones y servicios considerados críticos dentro de la entidad, que contribuyen a restablecer en el menor tiempo posible los servicios y operaciones con el apoyo de un plan de continuidad del negocio de las entidades.

Concluyendo lo anterior, el análisis de impacto del negocio, podrá ayudar a identificar dentro del marco de la seguridad de la información, las vulnerabilidades potenciales de la organización, podrá delimitar las actividades críticas que afectan el negocio y ayudará a la entidad a definir los planes adecuados de recuperación de los servicios que afectan el objeto del negocio; de otro lado la entidad podrán tener mayor información sobre el estado de los procesos contribuyendo favorablemente a mejorar la competitividad y proyectar estrategias adecuadas para una recuperación exitosa de la información.

Finalmente, es responsabilidad de las empresas del gobierno disponer de un recurso humano suficientemente capacitado y especializado, capaz de enfrentarse a los eventos inesperados que atentan con la operatividad, seguridad y disponibilidad de los sistemas de información y las comunicaciones.

 Hospital Departamental SANRAFAEL de Zarzal E.S.E. Transformando la atención en Salud	HOSPITAL DEPARTAMENTAL SAN RAFAEL DE ZARZAL E.S.E. VALLE DEL CAUCA Nit: 891900441-1	CÓDIGO: GI-SI -PL-05
		VERSIÓN: 03
		FECHA: 21/07/2025
		TRD:
	PLAN DE CONTINUIDAD DEL NEGOCIO PLAN DE CONTINGENCIA	PÁGINA: 15 de 15

BIBLIOGRAFIA

- ❖ Alexander, A., (2007). Diseño de un Sistema de Gestión de Seguridad de Información, óptica ISO 27001:2005, Alfaomega.
- ❖ Hiles, A., (2004). Business Continuity Best Practices, Connecticut: Rothstein Associates, Inc.
- ❖ ISO/IEC 27001:2006, Norma Técnica NTC-ISO/IEC Colombiana, Tecnología de la Información. Técnicas de Seguridad. Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos.
- ❖ ISO/IEC 27035, Information Technology. Security Techniques. Information Security incident imanagement
- ❖ ISO/IEC 27000, Information Technology. Security Techniques. Information Security Management Systems. Overview and Vocabulary
- ❖ ISO/IEC 27001, Information Technology. Security Techniques. Information Security Management Systems. Requirements
- ❖ ISO/IEC 27002, Information Technology. Security Techniques. Code of practice for information security management
- ❖ ISO/IEC 27005, Information Technology. Security Techniques. Information security risk Management
- ❖ ISO 22301:2012, Sistemas de Gestión y Continuidad del Negocio.
- ❖ ISO 27031 – DE198-13, Tecnología de la Información, Técnica de Seguridad, Directrices para la continuidad del negocio.

ELABORÓ		REVISÓ		APROBÓ	
Nombre:	Sandra Milena Rincón	Nombre:	Sandra Milena Rincón	Nombre:	Comité institucional de gestión y desempeño
Cargo:	Coordinadora de sistemas	Cargo:	Coordinadora de sistemas	Cargo:	Comité
Fecha:	02/12/2022	Fecha:	06/12/2022	Fecha:	06/12/2022
ACTUALIZA		REVISÓ		APROBÓ	
Nombre:	Aura Yineth Corrales O.	Nombre:	Sandra Milena Rincón	Nombre:	Comité institucional de gestión y desempeño
Cargo:	Ingeniera de sistemas	Cargo:	Coordinadora de sistemas	Cargo:	Comité
Fecha:	17/12/2023	Fecha:	18/12/2023	Fecha:	18/12/2023
ACTUALIZA		REVISÓ		APROBÓ	
Nombre:	Aura Yineth Corrales O.	Nombre:	Sandra Milena Rincón	Nombre:	Comité institucional de gestión y desempeño
Cargo:	Ingeniera de sistemas	Cargo:	Coordinadora de sistemas	Cargo:	Comité
Fecha:	21/07/2025	Fecha:	22/07/2025	Fecha:	