

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

CONTENIDO

1. INTRODUCCIÓN	3
2. OBJETIVOS	3
2.1. Objetivo general	3
2.2. Objetivos específicos	3
3. ALCANCE	4
4. MATERIALES, INSUMOS Y DISPOSITIVOS	4
5. MARCO LEGAL	4
6. ENFOQUE DIFERENCIAL	5
7. DEFINICIONES	5
8. DESCRIPCIÓN DEL PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	6
9. INFORMACION GENERAL	7
9.1. Servicios ofrecidos	7
9.2. Condiciones generales	7
9.3. Condiciones iniciales	7
10. PLAN DE RECUPERACION DE DESASTRES	8
10.1. Posible escenario	8
10.2. Centro de datos	8
10.3. Infraestructura de comunicaciones	8
10.4. Servidores	9
11. ROLES Y RESPONSABLES	9
12. NOTIFICACIÓN, EVALUACIÓN Y ACTIVACIÓN DEL DRP	10
12.1. Responsables del reporte del evento	10
12.2. Responsables de la evaluación del impacto del o de los incidentes	11
12.3. Activar el plan de contingencia	11
12.4. Posibles fallas o daños	11
12.5. Daño en las comunicaciones	11

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

12.6.	Daño en infraestructura de servidores	12
12.7.	Daño en Infraestructura de Bases de datos, Almacenamiento y copia ...	12
12.8.	Manejo de la crisis o contingencia	12
12.9.	Comunicados sobre la crisis o contingencia	13
12.10.	Actualización y mantenimiento del DRP	13
12.11.	Recursos mínimos para un plan de contingencia	13
13.	GLOSARIO	14
14.	CONTROL DE CAMBIOS.....	16
15.	APROBACIÓN.....	16

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

1. INTRODUCCIÓN

En la era digital actual, la infraestructura tecnológica no es solo un soporte, sino el motor crítico que permite la continuidad operativa, la protección de datos y la prestación de servicios. Sin embargo, este ecosistema está expuesto a diversas amenazas desde fallos de hardware y errores humanos hasta ciberataques y desastres naturales que pueden paralizar la organización en cuestión de segundos.

El presente Plan de Recuperación de Desastres Tecnológicos (DRP) se establece como el marco estratégico y operativo diseñado para minimizar el impacto de un evento disruptivo. Su objetivo principal es garantizar que, ante una contingencia grave, los sistemas de información y servicios críticos puedan ser restaurados en los tiempos y condiciones necesarios para salvaguardar la integridad de la institución.

2. OBJETIVOS

2.1. Objetivo general

Establecer el plan de recuperación de desastres tecnológicos (DRP) de Sistemas de Información y Tecnología de la ESE HOSPITAL SAN JUAN DE DIOS DE YARUMAL, en caso de la ocurrencia de un evento que impacte los servicios tecnológicos de la entidad, que afecte la Confidencialidad, Integridad y Disponibilidad de la información con el propósito de reestablecer dichas propiedades de la información.

2.2. Objetivos específicos

- Analizar posibles amenazas como fallos de hardware, ciberataques, errores humanos o desastres naturales.
- Determinar el impacto en los sistemas críticos de la organización.
- Establecer procedimientos para la restauración de sistemas, bases de datos y servicios clave.
- Garantizar la redundancia y respaldo de la información mediante copias de seguridad.

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

- Especificar el equipo de respuesta ante incidentes y sus funciones durante una recuperación.

3. ALCANCE

Comprender desde el despliegue de las metodologías utilizadas para la recuperación y estabilidad de los servicios y sistemas de información, a pesar de los desastres que perturben los procesos de la ESE HOSPITAL SAN JUAN DE DIOS DE YARUMAL. En consecuencia, poder estar prevenidos para enfrentar los incidentes y poder reintegrar las funciones y servicios con eficacia y eficiencia, es decir, atenuando el impacto de los eventos no deseados.

4. MATERIALES, INSUMOS Y DISPOSITIVOS

Dispositivos, documentación, servidores, materiales físicos y de sitio.

5. MARCO LEGAL

- **Ley 1523 de 2012 (Política Nacional de Gestión del Riesgo de Desastres):** es la norma fundamental que obliga a entidades públicas y privadas a gestionar el riesgo, lo que incluye la preparación ante desastres tecnológicos que puedan interrumpir el servicio.
- **Decreto 2157 de 2017 (Directrices para la Gestión del Riesgo):** adopta directrices obligatorias para la elaboración de planes de gestión del riesgo de desastres, incluyendo la identificación de escenarios de riesgo y medidas de recuperación.
- **Decreto 1072 de 2015 (Sistema de Gestión de Seguridad y Salud en el Trabajo):** en su artículo 2.2.4.6.25, obliga a las empresas a implementar, mantener y probar un plan de emergencias, que incluye la recuperación de infraestructura crítica.

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

- **Decreto 338 de 2022 (Gobernanza de la Seguridad Digital):** establece la necesidad de adoptar medidas técnicas y administrativas para la gestión de riesgos de seguridad digital, reportar infraestructuras críticas y responder a incidentes.
- **Ley 1273 de 2009 (Delitos Informáticos):** modifica el Código Penal y protege la confidencialidad, integridad y disponibilidad de la información, reforzando la necesidad de planes de recuperación ante ataques.

6. ENFOQUE DIFERENCIAL

El principio de enfoque diferencial reconoce que hay poblaciones con características particulares en razón de su edad, género, raza, etnia, condición de discapacidad y víctimas de la violencia, para las cuales el Sistema General de Seguridad Social en Salud ofrecerá especiales garantías y esfuerzos encaminados a la eliminación de las situaciones de discriminación y marginación. (Artículo 3, Ley 1438 de 2011).

La ESE Hospital reconoce la existencia de grupos poblaciones que por diferentes condiciones sociales, culturales, económicas y de salud requieren una especial atención, haciendo énfasis en la igualdad de oportunidades desde la diferencia, la diversidad y la no discriminación. Para ampliar información diríjase al protocolo de atención con enfoque diferencial **PT-09-001**.

7. DEFINICIONES

- **RTO (Recovery Time Objective - Objetivo de Tiempo de Recuperación):** el periodo de tiempo máximo permitido para que un proceso de negocio o sistema sea recuperado después de un desastre. Es el "reloj de arena" que indica cuánto tiempo podemos estar fuera de servicio.
- **RPO (Recovery Point Objective - Objetivo de Punto de Recuperación):** la cantidad máxima de datos (medida en tiempo) que la organización está dispuesta a perder. Define la frecuencia de los respaldos; por ejemplo, si el RPO es de 1 hora, no podemos perder más de una hora de transacciones.

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

- **MTPD (Maximum Tolerable Period of Disruption):** el tiempo máximo que un proceso puede interrumpirse antes de que el daño sea irreversible para la supervivencia de la organización.
- **Plan de Recuperación de Desastres (DRP):** conjunto documentado de políticas y procedimientos para recuperar y proteger la infraestructura tecnológica tras un incidente.
- **Plan de Continuidad de Negocio (BCP):** enfoque más amplio que asegura que los procesos críticos de la empresa sigan funcionando, mientras el DRP se enfoca en la tecnología.
- **Plataforma Tecnológica Crítica:** servidores, bases de datos, redes y aplicaciones esenciales cuyo fallo detiene la operación de la empresa.
- **Sitio Alternativo/Sitio de Recuperación:** ubicación física o en la nube diseñada para operar si el centro de datos principal se vuelve inaccesible.

8. DESCRIPCIÓN DEL PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS

El presente documento establece el Plan de Recuperación de Desastres Tecnológicos (DRP) para la ESE Hospital San Juan de Dios de Yarumal, con el fin de garantizar la continuidad de los servicios tecnológicos críticos ante la ocurrencia de eventos disruptivos. Este plan define los objetivos, el alcance, las estrategias de recuperación, los roles y responsabilidades del personal, así como los procedimientos de notificación, evaluación, activación y manejo de contingencias. Además, contempla la infraestructura tecnológica necesaria para responder eficazmente a incidentes que afecten la confidencialidad, integridad y disponibilidad de la información. A través de este DRP, se busca minimizar el impacto de desastres tecnológicos, restaurar los servicios en el menor tiempo posible y proteger los activos de información de la institución.

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

9. INFORMACION GENERAL

La ESE HOSPITAL SAN JUAN DE DIOS DE YARUMAL es una institución de segundo nivel de complejidad la cual cuenta con la sede principal y tres centros de salud dos en el área urbana y uno en la parte rural, también cuenta con puestos de salud en los corregimientos.

9.1. Servicios ofrecidos

- **Urgencias**
- **Hospitalización**
- **Cirugía**
- **Odontología**
- **Vacunación**
- **Programas de PYM**
- **Servicios de apoyo** (laboratorio, imágenes diagnósticas, Farmacia)
- **Consulta externa** (medicina general y especializada)
- **Servicios administrativos** (cartera, facturación, almacén, mantenimiento etc.)

9.2. Condiciones generales

El DRP está enfocado a la protección de la plataforma tecnológica que soporta los procesos misionales y de apoyo de la ESE.

9.3. Condiciones iniciales

- No se dispone de la infraestructura y recursos que soporten las estrategias de contingencia y recuperación para los sistemas críticos.
- Los funcionarios que ejecutan el plan, o sus suplentes, se encuentran disponibles y no han sido afectados por el desastre.
- El desastre no afectó simultáneamente el Centro de datos principal
- Solo el funcionario responsable activará el DRP.
- No se han realizado las pruebas de las estrategias y procedimientos al menos 1 vez al año.

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

- Los funcionarios no han participado en las pruebas y capacitaciones realizadas.
- Los Backups de las bases de datos e información se realizan de acuerdo a los procedimientos y cronogramas establecidos.

10. PLAN DE RECUPERACION DE DESASTRES

10.1. Posible escenario

Se refiera al o los posibles escenarios que se puede enfrentar la ESE.

10.2. Centro de datos

- Incendio
- Inundación
- Terremoto
- Perdida o daño en suministro eléctrico
- Daño en los sistemas enfriamiento (aire acondicionado)

10.3. Infraestructura de comunicaciones

- Daño o perdida de conexión en switches centrales
- Falla o perdida de conexión con el proveedor de internet
- Daño o perdida de conexión router central
- Daño o perdida de conexión con enlaces principales (internet, base datos, aplicativos etc.)
- Daño o perdida de conexión con las sedes
- Daño o perdida de conexión con firewall
- Daño o bloqueo de puertos de comunicación
- Virus informáticos
- Ataques o violaciones a la integridad de los datos o servicios de la ESE.

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

10.4. Servidores

- Daño o pérdida de conexión con base de datos (Oracle)
- Daño o pérdida de conexión de controlador de dominio (Virtualizado)
- Daño o pérdida de conexión con aplicativo hospitalario (XENCO)
- Daño o pérdida de conexión de equipos de almacenamiento (NAAS)
- Daño o pérdida de backup (base datos Oracle y NAAS)

11. ROLES Y RESPONSABLES

- DIRECTIVOS
- COORDINADOR DE SISTEMAS
- AUXILIARES DE SISTEMAS

Rol	Antes del evento	Durante el evento	Después del evento
Directivos	- Aprobar y participar en los procesos y divulgación de plan de recuperación de desastres tecnológicos	- Apoyar al personal de sistemas ante este tipo de eventos - Informar a todo el personal de la institución sobre el problema - Contactar con proveedores si es necesario	- Participar en las actividades de evaluación y mejora - Suministrar los recursos requeridos tanto de personal como equipos
Coordinador de sistemas	- Mantener actualizado el plan de recuperación de desastres tecnológicos - Gestionar los recursos necesarios - Mantener comunicación con los directivos sobre las contingencias que se han presentado	- Dar respuesta inmediata al evento, donde se debe evaluar la situación y activar plan de respuesta a dicha contingencia - Informar a las diferentes dependencias sobre la situación para que activen sus planes de contingencia - Informar a los directivos sobre la situación actual	- Realizar planes de mejoramiento de acuerdo a los eventos presentados para evitar futuros desastre o minimizar los riesgos y tiempos de respuesta - Informar a las diferentes áreas sobre el retorno a la normalidad del servicio - Informar a los directivos sobre el evento y poner en marcha planes de

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

		- Hacer el llamado al personal necesario para dar respuesta al evento y poder restablecer el servicio en el menor tiempo posible	mejora para evitar futuros problemas.
Auxiliares de sistemas	- Proponer o participar en planes de mejora - Coordinar actividades de entrenamiento, documentar y actualizar el DRP - Identificar las necesidades del área	- Participar en la solución de las contingencias que se presenten - Comunicar al coordinador sobre el evento - Ejecutar el plan ante eventos similares - Informar a las dependencias sobre la situación	- Participar en los planes o actividades de mejora

12. NOTIFICACIÓN, EVALUACIÓN Y ACTIVACIÓN DEL DRP

12.1. Responsables del reporte del evento

- El personal de la ESE debe reportar la pérdida o fallas en el servicio, por los medios disponibles por la entidad, tales eventos pueden ser:
 - No hay acceso XENCO
 - No hay internet
 - No hay acceso a los correos
 - No hay acceso a la telefonía
 - Cualquier evento que afecte el correcto funcionamiento del servicio
- Cualquier persona de la ESE debe informar cuando se presenta estas situaciones:
 - Suena la alarma contra incendios o hay un incendio en el centro de datos.
 - Hay inundación o agua en el piso del centro de datos.
 - Cualquier otro evento similar que afecte el centro de datos
- El personal de sistemas debe atender y monitorear los eventos que se presenten de acuerdo al plan como, por ejemplo:
 - Afectación del servicio a nivel general o parcial

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

- Ataque de virus informáticos
- Se detecta caída de los servicios
- Mal funcionamiento de la infraestructura tecnológica (servidores, base datos, Naas entre otros)
- Cualquier otro tipo de evento que afecte el correcto funcionamiento del servicio
- Afectación en las estaciones de trabajo de manera parcial o general

12.2. Responsables de la evaluación del impacto del o de los incidentes

El coordinador de sistemas y auxiliares, deben realizar un diagnóstico sobre el evento presentado, donde deben tener en cuenta:

- Tipo de incidente
- Impacto del incidente
- Tiempo estimado de solución del evento
- Aplicar el DRP u otras soluciones posibles

12.3. Activar el plan de contingencia

El coordinador define si activa o no el plan de contingencia, también debe informar a los directivos sobre el evento e impacto que tendrá, teniendo en cuenta lo siguiente:

- Asegurar la información de la base datos (Oracle) y de las NAAS
- Personal involucrado en el plan recuperación
- Verificar los servicios que están o no están funcionamiento
- Dar prioridad a los servicios esenciales
- Activar los servicios cuando se hagan pruebas de su correcto funcionamiento
- Proceder a dar solución de una oportuna

12.4. Posibles fallas o daños

El coordinador de sistemas en compañía de sus auxiliares deberá verificar y comprobar los daños en dicha contingencia

12.5. Daño en las comunicaciones

- Configurar o instalar switch de respaldo en caso de daño en uno o más de los switches principales (si se cuenta con switch de respaldo).

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

- Contactar con el proveedor de internet si la falla se presenta es en el enlace del proveedor
- Cargar copia de respaldo de la configuración del firewall en caso de falla

12.6. Daño en infraestructura de servidores

- Activar servidor de dominio de respaldo
- Activar servidor de base datos (ORACLE) de respaldo
- Activar servidor de aplicativo de respaldo (XENCO)

En caso de no contar con servidores de respaldo se debe solicitar a los directivos

12.7. Daño en Infraestructura de Bases de datos, Almacenamiento y copia

- Recuperar información desde las copias de seguridad, tanto para la base datos (**ORACLE**) y almacenamiento (**NAAS**).
- En caso de daño o pérdida de copias de seguridad tener una nube para respaldar las copias de la información crítica como lo es la base datos (**ORACLE**) y datos esenciales del equipo de almacenamiento (**NAAS**)

12.8. Manejo de la crisis o contingencia

El líder de sistemas se debe comunicar e informar a los directivos sobre el problema teniendo presente los siguientes aspectos

- Sistemas y servicios afectados
- Resultados del diagnostico
- Acciones realizadas o por realizar
- Tiempo estimado para poner en marcha el servicio
- Posibles riesgos a los que se enfrenta la entidad ante este tipo de desastres
- Decisiones que deben tomar los directivos ante este tipo de sucesos
- Los directivos deberán evaluar el problema y el impacto que puede tener en la prestación del servicio y se definirán acciones a tomar en conjunto con el equipo de sistemas
- Los directivos serán los encargados de informar en toda la entidad sobre el problema que se está presentando

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

12.9. Comunicados sobre la crisis o contingencia

- Se debe informar de manera rápida, precisa y constante sobre la problemática
- Siempre hablar con la verdad sobre el problema
- Al emitir reportes sobre la situación se debe ser lo más exacto posible
- Informar a las autoridades competentes sobre el tema si es necesario (cuando se trata de un ataque informático)

12.10. Actualización y mantenimiento del DRP

Es responsabilidad del líder de sistemas, la actualización y divulgación de dicho plan.

Se deberá actualizar cuando se presenten las siguientes condiciones

- Cuando hay cambios en las tecnologías o plataformas de la institución
- Cuando hay cambio en el personal encargado del DRP
- Cuando las auditorías lo ameriten
- Cuando las pruebas internas y externas por parte del personal de sistemas lo consideren
- Cuando la norma lo exija

12.11. Recursos mínimos para un plan de contingencia

- 1 servidor Hp Proliant DL 380 GEN10

Con las siguientes características para la base datos (ORACLE)

Procesador	Memoria RAM	Almacenamiento	Servicios
Intel Xeon Silver 4210R X 2	128 GB	1 TB SSD	Oracle Linux

- 1 servidor Hp Proliant DL 380 GEN10

Con las siguientes características para el aplicativo hospitalario (XENCO)

Procesador	Memoria RAM	Almacenamiento	Servicios
Intel Xeon Silver 4210R X 2	128 GB	1 TB SSD	- Windows Server 2022 - Controlador de dominio

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

- **1 servidor QNAP TS-431XeU de almacenamiento**

Con las siguientes características para las copias de seguridad

Procesador	Memoria RAM	Almacenamiento	Servicios
ARM Cortex– A15	4 GB	2 x 16 TB HDD	Copias se seguridad

- **2 SWITCH HP o CISCO base 1000 de 48 puertos**

Para poder reemplazar los equipos afectados o dañados

- **NUBE**

Para almacenar las copias seguridad de la base datos (**ORACLE**) por ser información crítica para la entidad.

- **FIREWALL**

Actualización del equipo (compra)

- **Notificación a las autoridades pertinentes (CSIRT Gobierno / COLCERT)**

Garantizar una **respuesta coordinada, oportuna y efectiva** ante incidentes de ciberseguridad que puedan afectar la infraestructura tecnológica o la información de la organización, cumpliendo con la normativa colombiana y las buenas prácticas de gestión de incidentes.

13. GLOSARIO

Switch: un switch de red, también conocido como conmutador, es un dispositivo que permite conectar varios dispositivos a una red. Esto permite que los dispositivos puedan compartir información y comunicarse entre sí.

Nube: la nube es un servicio de internet que permite almacenar, administrar y acceder a datos, aplicaciones y servicios desde cualquier dispositivo conectado a internet.

Firewall: un firewall es un dispositivo de seguridad que controla el tráfico de red que entra y sale de un dispositivo. Su objetivo es proteger la red interna de amenazas externas

Activo de información: se refiere al activo que contiene información o elementos relacionados con el manejo de la información (sistemas, soportes, edificios, personas y que se caracteriza por tener valor para la organización o entidad (ISO/IEC 27000).

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

Análisis del impacto al negocio: proceso del análisis de actividades las funciones operacionales y el efecto que una interrupción del negocio podría tener sobre ellas. (ISO 22300).

Continuidad del negocio: capacidad de la organización de continuar entregando productos y servicios a niveles aceptables predefinidos después de que ocurra un evento.

DRP: Plan de Recuperación ante Desastres de Tecnología, información documentada que define los procedimientos, estrategias, y roles y responsabilidades establecidos para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

Interrupción: Incidente, bien sea anticipado (ej: huracán) o no anticipados (ej. fallas eléctricas, 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 entidad.

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 de operación debido una vez presentada / tras la interrupción.

Plan de contingencia: define los procedimientos y medidas que se deben tomar para que las organizaciones puedan continuar operando en caso de una situación de desastre o emergencia.

Plataforma tecnológica crítica: hace referencia a los sistemas de información, servidores, bases de datos, sistemas de almacenamiento y respaldo, equipos y enlaces de comunicación que son esenciales para soportar los procesos y servicios de la entidad.

RAS: documento que relaciona las diferentes alternativas y estrategias potenciales para recuperar y mantener el servicio de tecnología ante un evento de interrupción.

RTO: tiempo máximo de interrupción tolerable para un proceso, servicio, proveedor, sistema de información o plataforma tecnológica.

	E.S.E. HOSPITAL SAN JUAN DE DIOS DE YARUMAL NIT 890.981.726-6		
	PLAN DE RECUPERACIÓN DE DESASTRES TECNOLÓGICOS	PROCESO DE SISTEMAS DE INFORMACIÓN	CÓDIGO: PL-20-004
			VERSIÓN: 02
			FECHA: 24/03/2026

RPO: cantidad de datos o información, en términos de tiempo, que tolera perder un proceso o servicio cuando se presenta un evento alterador del normal funcionamiento.

14.CONTROL DE CAMBIOS

Fecha	Versión	Páginas Afectadas	Descripción del contenido
29/04/2025	01		Creación documento original
24/03/2026	02	Todo el documento	Actualización del documento

15.APROBACIÓN

Actualización	Revisó	Aprobación
Gustavo Adolfo Gómez López	Yenny Alexandra Herrera Agudelo - Ana Maria Yepes Torres	Daniel Alcides Vergara Tobón
Auxiliar de sistemas	Profesional de Calidad - Apoyo de calidad	Gerente