Plan de Recuperación ante Desastres

Medical Solutions Colombia SA

1. Objetivos

Este documento define el procedimiento para identificar las actividades críticas de la organización y los riesgos a los que se ven expuestas con el fin de determinar planes de acción que permitan una correcta recuperación y continuidad de las mismas ante una interrupción.

El objetivo de un plan de recuperación ante desastres es garantizar que se pueda responder a un desastre u otra emergencia que afecte a los sistemas de información y minimizar el efecto en el funcionamiento del negocio. Este documento debe estar resguardado en un lugar seguro y accesible.

Los principales objetivos de un plan de recuperación de desastres, son:

- Minimizar las interrupciones a las operaciones normales.
- Limitar el alcance de la interrupción y el daño.
- Minimizar el impacto económico de la interrupción.
- Establecer medios alternativos de operación por adelantado.
- Capacitar al personal con procedimientos de emergencia.
- Proporcionar una restauración rápida y sin problemas del servicio.

2. Alcance

Este plan cubre todos los componentes de tecnología que dan soporte a los productos y servicios ejecutados y provistos por Medical Solutions Colombia SA.

Los servicios y productos de tecnología provistos por proveedores y provenientes de ambientes externos se encuentran involucrados en este proceso y contempladas sus acciones para garantizar la continuidad.

La revisión, y en caso de ser necesario, la adecuada actualización de este plan debe realizarse al menos una vez al año.

3. Definiciones

Incidencia: un único evento o serie de eventos de seguridad de la información inesperados o no deseados, que tienen una probabilidad significativa de comprometer las operaciones empresariales y de amenazar la seguridad de la información.

Contingencia: acción correctiva frente a una incidencia.

Procedimiento: normas y/o pasos predefinidos para actuar frente a una situación, normalmente establecido mediante políticas internas.

Plan: hace referencia a este documento en general y lo que afecta.

Plan de Continuidad de Negocios (BCP): Documento donde se detalla el proceso para continuar las operaciones comerciales críticas durante y después de una interrupción del negocio.

Plan de Recuperación de Desastres (DRP): Documento donde se detalla el proceso de recuperación de las herramientas informáticas y tecnológicas de la organización afectadas por un desastre. Es el aspecto tecnológico del BCP.

Objetivo de punto de recuperación (RPO): es la cantidad aceptable de pérdida de datos medida en el tiempo. Por ejemplo, si ocurre un desastre a las 13:00 y el RPO es de una hora, el sistema debe recuperar todos los datos que estaban en el sistema antes de las 12:00. La pérdida de datos abarca solo una hora, entre las 12:00 y las 13:00.

Objetivo de tiempo de recuperación (RTO): Es el tiempo que toma después de una interrupción para restaurar un proceso de negocio a su nivel de servicio. Por ejemplo, si ocurre un desastre a las 12:00 y el RTO es de dos horas, el proceso de DR debe restaurar el proceso de negocios al nivel de servicio aceptable para las 14:00. Se considera el peor escenario, los tiempos máximos se estipulan en caso que resulte necesario algún reproceso, tendrán precedencia los sistemas más críticos.

4. Vigencia

Este plan entrará en vigencia a partir del día 14 de Octubre de 2021

5. Estrategia de Recuperación

La estrategia de recuperación comienza desde el procedimiento de manejo de incidencias, el cual detecta, escala los requerimientos y define si es necesario iniciar el plan de recuperación y/o el plan de Emergencia y Contingencia.

5.1. Procedimiento de manejo de incidencias

El procedimiento de manejo de incidencias que afectan a las tecnologías que dan soporte al servicio proveído por Medical Solutions Colombia SA comienza cuando se detecta alguna falla en el sistema que impida el correcto funcionamiento de los usuarios en la plataforma. Si la incidencia afecta la integridad de las personas, entonces se activa el plan de Emergencia y Contingencia. Si la incidencia no se puede resolver en el primer nivel de ayuda, entonces se realiza el escalamiento al encargado de continuidad operacional o Líder del Plan de Continuidad.

El orden en el cual se realiza el escalamiento de las incidencias se puede ver en la Tabla 1. Este escalamiento se realiza de forma interna. El cliente se debe contactar con el primer nivel de escalamiento de incidencias.

N°	Encargado	Medio de Contacto	Rol	Datos de Contacto
1	Marcia Venegas	Sistema "Adereso" (adere.so)	Servicio al Cliente	**Público:** https://www.medismart.live/cl/index.html#ayuda +56953694225 **Interno:** marcia.venegas@medismart.live +56981680295
2	Diego Álvarez	Correo	Oficial de Seguridad de Información y Administrador de Plan de Continuidad de Negocios	diego.alvarez@medismart.live +56990992229
3	Cristián Farías	Correo	Encargado de Tecnología	cristian.farias@medismart.live +56950970882

Tabla 1. Orden de escalamiento de incidencias

5.2 Procedimiento de operaciones de reColombia SAldo

Para garantizar que se puedan realizar tareas operativas esenciales de procesamiento de datos después de la interrupción, el equipo de Medical Solutions Colombia SA realiza las siguientes actividades:

- Se mantienen los reColombia SAldos físicos(.bacpac) de forma mensual (AZURE bajo el plan de recuperación “on demand” permite un punto de recuperación de la base de datos de cualquier hora dentro de 7 días.
- Se cuenta con reColombia SAldo de todas las componentes(código fuente) del sistema en caso de ser necesario levantar un nuevo servicio.
- Vultr cuenta con snapshots para restauración en un tiempo estimado de 4 horas. Backup de dos días.

5.3. Procedimientos de acciones de recuperación.

Para facilitar la rápida restauración de un sistema de procesamiento de datos después de un desastre. Todo plan de recuperación ante desastres debe comenzar con la siguiente lista de actividades:

A. Notificar al encargado de continuidad operacional o Plan de Continuidad.
B. Notificar a la alta dirección.
C. Contactar y configurar el equipo de recuperación de desastres.
D. Determinar el grado de desastre.
E. Implementar un plan de recuperación de aplicaciones adecuado en función del alcance del desastre.
F. Monitorear el progreso.
G. Ponerse en contacto con el sitio de copia de seguridad y establecer horarios. Ponerse en contacto con el resto del personal necesario, tanto el usuario como el equipo técnico.
H. Ponerse en contacto con los proveedores, tanto de hardware como software.
    a. En caso de ser necesario, notificar a los usuarios sobre la interrupción del servicio, lo que se determinará en base a el efecto que tenga el incidente sobre la experiencia de los mismos.

5.4. Procedimiento de recuperación ante la indisponibilidad del sistema

En caso de que el servicio no esté recibiendo peticiones se debe:

1. Ingresar a consola de proveedor afectado (VULT-R, Sonda, PayQ, Vonage, adere.so).
2. Revisar alertas y alarmas configuradas en consola.
3. Identificar componentes sin funcionamiento. Si el componente caído es el servicio de base de datos, se debe ir al procedimiento de recuperación ante caída de la base de datos.
    a. Revisar créditos asignados a cada componente.
    b. Realizar imagen de seguridad del componente caído.
    c. Intentar reiniciar el componente caído.
4. Si no hay componentes caídos, pasar a procedimiento de recuperación ante la falla de software.
5. Revisar fallas en grupo de auto escalamiento (que debe levantar instancias de forma automática)

6. En caso de que el componente no pueda ser reiniciado, se debe restaurar desde su último snapshot.
    a. Si el snapshot no soluciona el problema, se debe restaurar desde la última imagen estable de la solución.
7. Realizar pasos 2 a 6 hasta solucionar el problema.
8. Se notifica al responsable operacional.
    a. En caso de ser pertinente, se notifica del suceso al usuario final acerca del restablecimiento del servicio y/o medidas tomadas.

5.5. Procedimiento de recuperación ante falla en software

Este procedimiento solo se puede ejecutar si el procedimiento de recuperación ante la indisponibilidad del sistema identifica que no existe componente caído. Todo componente debe estar activo, indicando que es un error del software y no de acceso al sistema.

Pasos a seguir:

1. Contactar a Cristián Farías y al equipo de desarrollo y de operaciones.
2. Realizar reColombia SAldo extraordinario de la base de datos.
3. Realizar snapshot del ambiente productivo.
4. Configurar base de datos en ambiente de QA.
5. Revisar los logs del sistema para identificar problemas.
6. Si problema está relacionado a alguna actualización reciente, se debe restaurar software a la versión previa en el ambiente QA
    a. Si se corrige un problema en ambiente QA, entonces se debe corregir el software en dicho ambiente, realizando hotfix.
    b. Se ejecutan las pruebas unitarias de la solución.
    c. Si todas las pruebas están correctas y la solución, en ambiente QA, está operativa, entonces se realiza un paso a producción.
    d. Se realizan nuevas pruebas unitarias que eviten que el error se repita en el futuro.
7. Si el problema está relacionado a alguna configuración del sistema,
    a. Replicar los snapshots del ambiente productivo en un ambiente QA.
    b. Realizar pruebas de configuración para identificar problemas.
    c. Corregir problema en ambiente QA.
    d. Realizar pruebas unitarias de la solución.
    e. Realizar pruebas de usuario.
    f. Si no hay errores, se debe realizar paso a producción. En caso contrario, iterar punto 7.
    g. Realizar configuraciones en ambiente productivo.
    h. Documentar el error.
8. Se notifica al responsable operacional.
    a. En caso de ser pertinente, se notifica del suceso al usuario final acerca del restablecimiento del servicio y/o medidas tomadas.

5.6. Procedimiento de recuperación ante caída de la base de datos

1. Contactar al equipo de desarrollo y de operaciones.
2. Realizar reColombia SAldo extraordinario de la base de datos.
3. Realizar snapshot de los servidores de base de datos.
4. Restaurar un ambiente de QA de la base de datos. En dicho ambiente revisar que la base de datos tenga eColombia SAcio disponible en disco .
    a. Corregir eColombia SAcio si falta.
    b. Revisar logs de la base de datos.
    c. Revisar alertas de ambiente de datos.
    d. Identificar y corregir problemas en base de datos.
    e. Realizar pruebas en ambiente QA. Si fallan las pruebas, volver al punto 4.a.
    f. Realizar paso a producción de modificaciones.
5. Si la base de datos no puede ser corregida, se debe restaurar la última versión reColombia SAldada
6. Se notifica al responsable operacional.
    a. En caso de ser pertinente, se notifica del suceso al usuario final acerca del restablecimiento del servicio y/o medidas tomadas.

6. RTO y RPO

Se definen los siguientes valores de RTO y RPO para los procesos críticos y que comprometen la operación de la plataforma:

RTO: 5 Horas
RPO: 1 Hora

7. Pruebas del plan

El DRP es validado mediante el desarrollo de un ejercicio de prueba de los planes y la tecnología complementaria. Éste se lleva a cabo al menos una vez al año o luego de cambios significativos en la tecnología u organización.
Una vez que se completa el DRP, el coordinador y gerente del equipo de recuperación deben firmar el "Sign Off" (informe de resultado de pruebas) para garantizar que los componentes principales están suficientemente documentados.

8. Versionado

Confeccionado por	Diego Álvarez
Código de documento	DRP.V1
Versión	V1
Fecha de última actualización	12/10/2021
Revisado por	
Aprobado por	