DIXHI COMPANY SAS

TOP UP, BILLETERA DIGITAL

Plan de continuidad y Contingencia

2023

La Billetera para estar activos

www.topup.com.co

Tabla de contenido

1. Objetivos

El objetivo de este plan es implementar mecanismos, procedimientos basados en personas, infraestructura, tecnología, procesos, y cultura organizacional que permitan asegurar dentro de los parámetros consensuados con nuestros mandantes y clientes internos la normal operación del negocio en situaciones extremas.

Los procesos críticos negocio sobre los cuales se implementarán los controles antes mencionados son los siguientes:

1. Aumentar la confianza por parte de los clientes actuales y potenciales de DIXHI COMPANY SAS.
2. Asegurar que los Riesgos de Continuidad del Negocio que sean valorados como críticos, cuenten con controles implementados.
3. Lograr el cumplimiento del programa de capacitación de Continuidad del Negocio por parte de los colaboradores.
4. Asegurar el cumplimiento de los requisitos legales vigentes aplicables, identificados en la matriz de requisitos legales.
5. Reducir la probabilidad de caída de los procesos y servicios críticos, gracias a la implementación de controles eficaces.
6. Asegurar la recuperación de los procesos y servicios críticos de acuerdo con los parámetros de recuperación definidos.
7. Velar por el óptimo funcionamiento de sus servidores, sistemas y plataforma donde opera su principal producto TOP UP, Billetera digital.
8. Garantizar la respuesta a tiempo a sus colaboradores, proveedores, aliados, y usuarios sobre las novedades que se presenten en la operación.

2. Alcance

Para DIXHI COMPANY SAS el compromiso con la continuidad del negocio es primordial en todas las áreas que compone nuestra empresa.

- Área de tecnología que son quienes responden por el desarrollo y ejecución correcta de nuestro producto TOP UP, Billetera digital.
- Área financiera, responsables por transacciones y movimientos de nuestra billetera digital.

- Área de operaciones, responsables por vigilar que la operación y funcionamiento de la billetera esté dentro de lo requerido por los clientes y usuarios. Trabajando de la mano con el equipo de tecnología.
- Área legal, quien nos respalda en todo proceso legal de carácter urgente y prioritario.
- Área comercial, responsable por ser la cara ante nuestros clientes y usuarios, brindándole tranquilidad y seguridad ante cualquier novedad que se presente.

3. Vigencia

Su vigencia será a partir de 01/03/2023.

4. Responsabilidades

La empresa definió diferentes roles y responsabilidades.

Comité de Crisis

- Evaluar la contingencia detectada y tomar, en consecuencia, la decisión final de activar o no un determinado procedimiento de contingencia o una serie de ellos.
- Evaluar el curso de la contingencia a fin de establecer nuevas necesidades de activación.
- Evaluar el curso de la contingencia a fin de establecer la desactivación de un determinado procedimiento o un conjunto de ellos.
- Evaluar el curso de la contingencia y tomar la decisión sobre la finalización de la misma con la posterior notificación sobre la vuelta a la “normalidad”.
- Mantener una fluida comunicación con los coordinadores de Recuperación del Negocio a fin de que puedan mantener informado al comité y que puedan recibir las instrucciones para cada caso.

Líder del equipo del Plan de Continuidad

- Discernir con criterio de negocio y operación la crisis en cuestión y es el responsable de activar el Plan de Contingencia.
- Contar con la autoridad y el conocimiento necesario para administrar la crisis.
- Definir el responsable de ejecución del backup y hacer seguimiento de su efectividad.

- Asegurarse de que se encuentren actualizados los contenidos del plan.
- Informar al Comité de Crisis sobre nuevas necesidades asociadas al plan.
- Identificar nuevos escenarios de riesgo potenciales.
- Coordinar las pruebas del plan de contingencias.

Miembros del equipo de Continuidad

- Mantener fluida comunicación con el comité de crisis informando el curso de la contingencia.
- Mantener fluida comunicación con el comité de crisis para recibir instrucciones y difundirlas a las líneas.
- Asegurarse de que la restauración se lleve a cabo en forma efectiva y en función a las necesidades de información de las diferentes partes.
- Informar y monitorear necesidades especiales y/o desvíos.
- Asegurarse de que el mapa de proceso se ejecuta conforme a lo establecido en el presente documento.

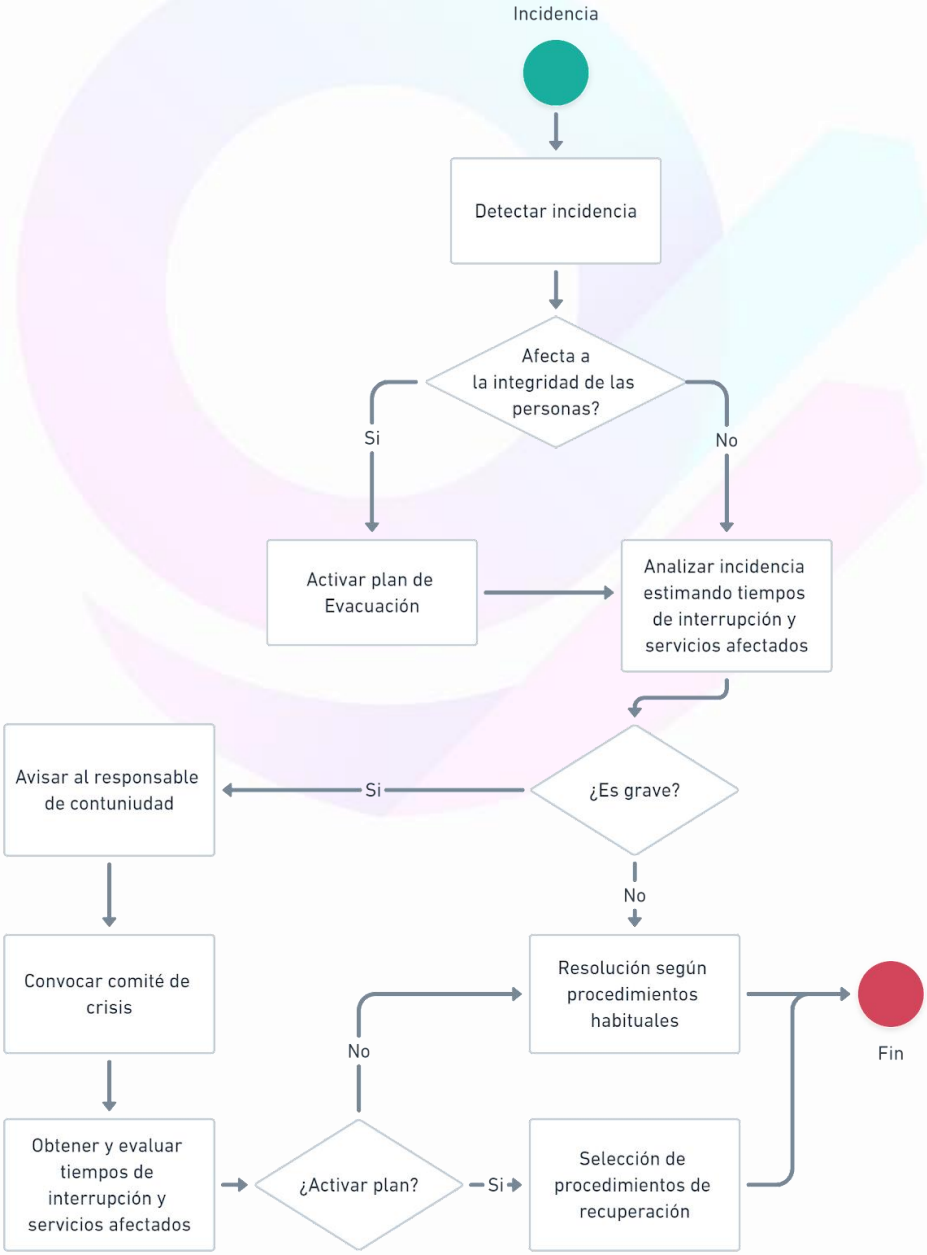
Rol	Área	Nombre y Contacto
Comité de Crisis	CEO + Business Manager	Marcela Santiago - 3218947395
Líder del equipo		Eder Chavez - 3057211567
Miembros del equipo de continuidad	Tecnología	Donna López - 3006400851
	Soporte IT	Samuel De La Hoz - 3013540830
	Operaciones	Eder Chavez - 3057211567
	Recursos Humanos	Maira Hernández - 3234670890
	CFO	Maira Hernández - 3234670890

5. Estrategias de recuperación

Se dictaminan algunas estrategias de recuperación para diversos incidentes.

Recurso crítico	Escenario de incidente	Estrategias de recuperación
Personas con responsabilidades en actividades criticas	Indisponibilidad total del personal	1. Formación multidisciplinar a través de webinars 2. Documentar actividades críticas 3. Separar tareas críticas
Proveedores	Indisponibilidad total ante caída de proveedores críticos	1. Contacto con proveedores alternativos 2. Envío y almacenamiento de recursos críticos en ubicaciones alternativas.
Información	Indisponibilidad de base de datos	1. Copias de seguridad 2. Procedimientos de recuperación 3. Redundancia de copias del plan de recuperación

6. Procedimiento



6.1. Procedimiento de recuperación ante indisponibilidad total de suministro eléctrico.

Nuestros servidores son tercerizados por ende en caso de fallar el suministro eléctrico procedemos de la siguiente manera:

- Notificar a la administración del edifico donde funcionan nuestras oficinas.
- La administración del edificio notificará a la empresa prestadora de servicio para reportar la falla y determinar las causas de esta. En caso de no recibir respuesta, dispondremos de un técnico especializado para solucionar este tipo de inconvenientes.
- Si el percance supera el tiempo establecido de espera, pactado por la gerencia general de 30 minutos, nuestro personal podrá desplazarse y desarrollar sus funciones desde cualquier lugar siempre y cuando tenga acceso a fluido eléctrico y conexión a internet.

6.2. Procedimiento de recuperación ante indisponibilidad total del servicio de Proveedor Nube (server principal).

Ante una indisponibilidad total del servicio del proveedor de nube, se deben seguir los siguientes pasos para recuperar el servicio:

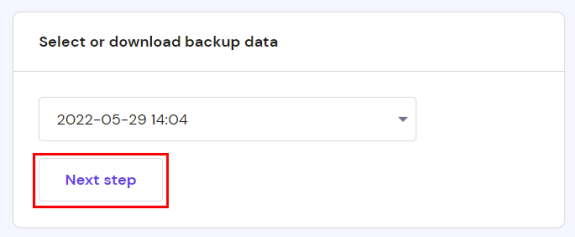
- Comunicarse con el proveedor de nube: Es importante contactar al proveedor de nube lo más rápido posible para que pueda investigar la causa del problema y proporcionar información actualizada sobre el estado del servicio.
- Verificar la red y la conectividad: Verifique si hay algún problema en la conexión de red. Asegúrese de que los enrutadores, los switches y los firewalls estén funcionando correctamente.
- Verificar la integridad de los datos: Verifique si los datos están intactos y no se han corrompido. Esto puede incluir realizar una copia de seguridad de los datos.
- Considerar la recuperación de datos: Si se ha producido una pérdida de datos, se debe considerar la recuperación de datos a través de la restauración de una copia de seguridad o de la recuperación de datos desde una ubicación secundaria.

- Planificar la recuperación: Planifique la recuperación del servicio en función de la criticidad del servicio y de las necesidades del negocio. Esto puede incluir la restauración del servicio en una ubicación secundaria o la implementación de una solución de recuperación ante desastres.
- Restaurar el servicio: Restaure el servicio siguiendo el plan de recuperación. Asegúrese de probar completamente el servicio antes de restablecer la conectividad con los usuarios finales.
- Monitorear el servicio: Monitoree el servicio para asegurarse de que se esté ejecutando correctamente y de que no haya problemas adicionales.

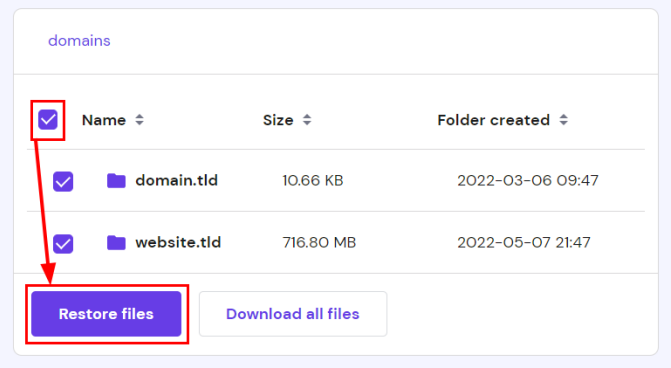
6.3. Procedimiento de recuperación ante indisponibilidad total de la conexión a enlaces de red.

El administrador de hosting nos proporciona copias diarias de seguridad de todos nuestros componentes y servicios (Archivos, Base de datos, dominios, etc.).

En el panel de administración se busca la opción “copias de seguridad” o “Backup”, una vez allí, se listan todos los tipos de copias de seguridad (archivos o bases de datos) que se realizaron.



Entonces, dependiendo de lo que se necesite restaurar selecciona la copia más reciente y procedemos a realizar los pasos estipulados por el administrador de hosting.



Al iniciar el proceso de restauración este dura un tiempo dependiendo del tamaño del componente a restaurar.

Ante la indisponibilidad total de la conexión a enlaces de red de un servidor de hosting, la empresa proveedora del servicio de hosting seguirá los siguientes pasos:

- Detectar el problema: El personal encargado debe detectar y verificar que el problema se debe a la indisponibilidad de la conexión a enlaces de red.
- Aislar el problema: Es necesario aislar el servidor afectado para evitar que el problema se propague a otros servidores y sistemas de la red.
- Notificar a los usuarios: el administrador del hosting nos debe comunicar sobre la situación y proporcionar una estimación del tiempo de recuperación.
- Realizar un diagnóstico: Se debe realizar un diagnóstico para determinar la causa del problema y su ubicación.
- Realizar reparaciones: Una vez que se haya determinado la causa del problema, se deben realizar las reparaciones necesarias.
- Realizar pruebas de conexión: Una vez realizadas las reparaciones, se deben realizar pruebas para asegurarse de que la conexión a enlaces de red del servidor está funcionando correctamente.
- Restaurar el servicio: Si las pruebas de conexión son exitosas, se puede restaurar el servicio y notificarnos sobre la solución.
- Investigación y análisis: Después de que se haya restaurado el servicio, es importante que el administrador de hosting junto a nosotros realicemos una investigación y análisis detallados de la causa del problema y tome medidas para evitar que se vuelva a producir en el futuro.

6.4. Procedimiento de recuperación ante indisponibilidad total del personal crítico.

- Levantar requerimientos de personal según área y enviarlos al área de RR.HH.
- Publicar ofertas de empleo en para reclutar nuevos candidatos o bien buscar un reemplazo interino.
- Realizar una contratación extraordinaria que facilite la velocidad de aprobación o rechazo del candidato por parte de la alta gerencia.

6.5. Procedimiento de recuperación ante indisponibilidad parcial del personal.

- Formación constante sobre el proyecto a toda el área de tecnología.
- Disponibilidad constante de personal para dar soporte a clientes y/o usuarios con novedades.
- Posibilidad de hacer coberturas internas, en cada área existe más de un colaborador con el fin de cubrir y asumir tareas en caso de ausencia.
- Contrataciones extraordinarias o FreeLancer.

6.6. Procedimiento de recuperación ante indisponibilidad parcial de sistemas operativos/base de datos.

Ante una indisponibilidad parcial de sistemas operativos/base de datos, el primer paso sería evaluar el alcance y la gravedad del problema. Para ello, se revisan los registros y las alertas del sistema para identificar el origen del fallo y determinar qué sistemas y servicios están afectados.

Luego, se llama al servidor de hosting y define las tareas y responsabilidades de cada uno de los miembros.
inmediatamente se procede a la recuperación de los sistemas y servicios afectados siguiendo los siguientes pasos:

Establecer un plan de contingencia que permita minimizar el impacto en los usuarios y garantizar la integridad de los datos.

Restaurar los servicios esenciales y críticos tan pronto como sea posible.

Identificar y solucionar la causa raíz del problema para evitar que se repita en el futuro.

Verificar que los sistemas y servicios estén completamente restaurados y que funcionen correctamente.

Comunicar a los usuarios y al equipo de soporte sobre el progreso y el estado de la recuperación y proporcionar información actualizada sobre cualquier posible impacto en los servicios.

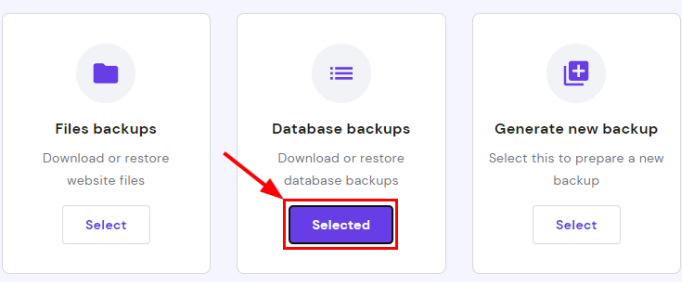
Realizar un análisis posterior al incidente para evaluar el rendimiento del equipo de recuperación de emergencia y para identificar oportunidades de mejora en los procesos de recuperación.

por último, documentar el incidente y revisar el plan de continuidad del negocio para asegurar que está actualizado y se puede aplicar de manera efectiva en futuras situaciones similares.

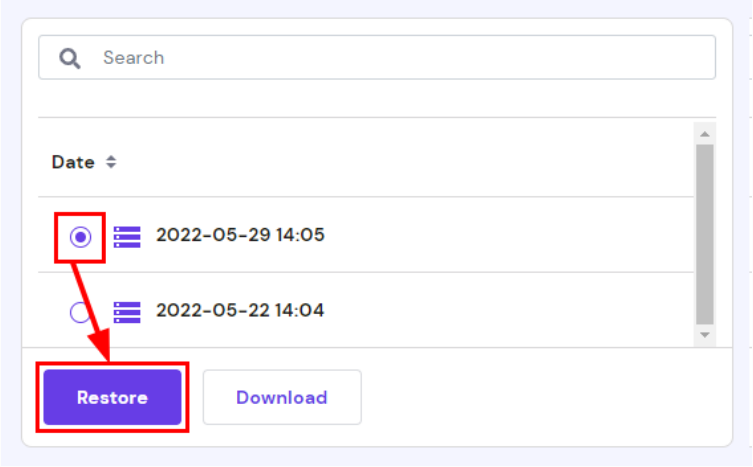
Restauración de Backup de Base de datos

Así como el administrador de hosting permite realizar copias de seguridad de los sitios web, también permite realizar copias de seguridad de las bases de datos e información dentro de ella.

El administrador de hosting permite seleccionar en el panel la opción de restaurar bases de datos.



selecciona la fecha de la copia, (Siempre es recomendable seleccionar la misma fecha que selecciono para la restauración del sitio web o la más reciente.) restauramos la base de datos.



6.7. Procedimiento de recuperación ante siniestros y catástrofes.

- Nuestras bases de datos y hosting cuentan con copias de seguridad ubicadas en diferentes países, con el fin de poder tener recuperación de la información ante cualquier eventualidad.
- Para nuestro centro de operaciones, toda nuestra información sobre el funcionamiento está respaldada con copias de seguridad, con la finalidad de acceder a esta desde cualquier lugar, desde cualquier dispositivo.
- El proyecto podrá ejecutarse desde cualquier ubicación y asi permitir la continuidad del mismo.

7. Mantenimiento del plan

Difusión y formación.

DIXHI COMPANY SAS ha definido un Plan de formación y concientización, que tiene por objetivo identificar el tipo de necesidades formativas que son requeridas y qué estrategia de comunicación es la más adecuada.

A partir de este esquema se desarrollará la programación de acciones formativas concretas en diversos entornos:

- En el de dirección y supervisión.
- En el de ejecución y operación.

DIXHI COMPANY SAS utilizará diversos medios para la impartición efectiva de talleres formativos, como por ejemplo, la realización de un curso de e-learning y la actualización y difusión de documentos relacionados, como por ejemplo la Política de Seguridad de la Información.

Los responsables claves (key user) son adecuadamente formados y concientizados acerca de los diferentes conceptos que contempla la continuidad de negocio (riesgos, medidas preventivas, detección temprana de incidencias, etcétera).

Mejora, actualización y puesta al día.

El plan de Continuidad de Negocio de **DIXHI COMPANY SAS** será revisado y actualizado durante **marzo** de cada año.

El líder del equipo de continuidad es el responsable de mantener al día este Plan y sugerir la incorporación de nuevos escenarios, planes y procesos en el plan.

Plan de pruebas.

Una vez actualizado el Plan de Continuidad de Negocio, el Administrador del Plan deberá establecer el Plan de Pruebas del Plan de Continuidad de Negocio, su contenido y la fecha más probable para realizar dichas pruebas.

Las acciones de activación, gestión y desactivación (procesos ante crisis) del Plan deben ser probadas con, al menos, la prueba de una de las acciones de continuidad contempladas en el presente.

Participantes de la prueba.

- Líder de Equipo de Continuidad.
- Miembros del equipo
- Usuarios de los procesos de negocio alcanzados por el Plan
- Usuarios de procesos ante crisis, designados por miembros del equipo de Contingencia.

Documentación respaldatoria de la prueba.

A los efectos de certificar la realización y resultados de la prueba del Plan, el Líder del Plan debe generar un informe sobre la misma, debiendo ser tomado en conocimiento por el CEO y el Comité de Seguridad.

Dicho informe debe nutrirse de la documentación de los resultados de la prueba que verifiquen el funcionamiento y efectividad del plan diseñado.

8. Versionado

Elaborado por:	Eder Chavez Cervera
Código de documento:	Código - 001
Versión:	v1
Fecha última de actualización:	03/04/2023
Revisado por:	Marcela Santiago Rizo
Aprobado por:	Marcela Santiago Rizo
Comunicado a:	Todas las áreas involucradas en la operación de la billetera digital.