HOUSERS
SMART INVESTMENT

Política de continuidad del negocio

1. Introducción

El propósito del Plan de continuidad de servicios de TI es definir con precisión cómo HOUSERS recuperará o continuará la operación de servicios de TI, aplicaciones, sistemas o componentes en el nivel acordado en los requerimientos de negocio.

Este plan se aplica a todas las actividades críticas dentro del alcance del Sistema de gestión de continuidad de servicios de TI.

Los usuarios de este documento son todos los miembros del personal, tanto internos como externos, que cumplan una función en la continuidad de servicios de TI.

2. Responsabilidad por la aplicación de la Política de continuidad del negocio

Los equipos de trabajo, sus actividades e integrantes están conformados según el siguiente cuadro:

Equipos	Funciones	Integrantes
Equipo Director	Dirigir las actividades durante la contingencia y recuperación. · Análisis de la situación · Activación o no del plan de recuperación · Seguimiento del proceso de recuperación · Evaluación de los daños	CTO (líder) DT (suplente) Responsable de sistemas
Equipo de Recuperación	Restablecer todos los servicios principales de TI que son: • Servicio de base de datos MariaDB • Servicio API • Servicio web front • Servicio web admin • Servicio web blogs • Servicio correo • Microservicio de gestión de comunicaciones • Microservicio de gestión documental • Microservicio de pagos • Microservicio de notificaciones	DT (líder) Responsable de sistemas (suplente) Responsable de Desarrollo de Software Asistentes de Desarrollo de Software

	• Servicio de almacén de archivos de oficina.	
Equipo de Pruebas	Realizarán las pruebas de verificación de operación de los servicios principales de TI.	Jefe de Desarrollo de Software Asistentes de Desarrollo de Software

3. Identificación de incidentes

La evaluación de riesgos evalúa el nivel de la amenaza (es decir, incidente disruptivo) y el hasta dónde HOUSERS es vulnerable a esa amenaza. La evaluación de riesgos se implementa a través del Cuadro de evaluación y tratamiento de riesgos. El proceso de evaluación de riesgos es coordinado por el Director Técnico y la evaluación de riesgos para servicios individuales es realizada por los responsables de los servicios.

3.1. Niveles de categorización de incidentes:

Consecuencia insignificante	1	La duración del incidente disruptivo no afecta significativamente las finanzas, las obligaciones legales o contractuales o el prestigio de la organización.
Consecuencia aceptable	2	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización, pero ese daño todavía es aceptable teniendo en cuenta su magnitud y circunstancias específicas.
Consecuencia mayor	3	La duración del incidente disruptivo provoca daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización y ese daño no es aceptable por su magnitud y circunstancias específicas.
Consecuencia catastrófica	4	La duración del incidente disruptivo provoca grandes daños sobre las finanzas, las obligaciones legales o contractuales o el prestigio de la organización que le harán perder la mayor parte de su capital y/o tendrá que cancelar sus operaciones en forma permanente.

3.2. Tipos de alertas

1. Alertas derivadas de Monitorizaciones de servicios
    a. Caída o ralentización del nivel de respuesta del servidor por ataque de Denegación de servicio
    b. No respuesta del servidor por caída de la conectividad del isp[1]
    c. Fallo en la conectividad del API con LemnonWay
    d. Bloqueo del sistema de BD
    e. Fallo en alguno de los microservicios alojados en el entono de Amazon WS**[2]
    f. Caída del servidor web por fallo de HW
2. Alertas derivadas de monitorizaciones de seguridad activa
    a. Notificaciones del centro de alerta temprana
    b. Alertas derivadas de auditorías periódicas de seguridad.
3. Alertas derivadas del error en funcionalidades del a plataforma
    a. asociadas a la operativa de los inversores

[1] **Datos del ISP**: Unelink Telecom S.A. (https://www.unelink.es). Proporciona la infraestructura de servidores que soporta los siguientes servicios:
• API
• MariaDB
• Web front
• Web admin
• Cpanel para alojar los diferentes blogs y el correo de la empresa
Para ello se dispone de 3 servidores dedicados virtualizados a través de Proxmox, lo que permite montar un cluster de alta disponibilidad.
Adicionalmente Unelink también proporciona a Housers los siguientes servicios:
• Back-up de datos en sus propios servidores, en nodos separados del nodo Housers
• Gestión de dominios
• Gestión de certificados SSL

[2] **Amazon WS:** por su parte, Amazon WS proporciona alojamiento en sus sistemas a 4 microservicios muy concretos de la plataforma:
- Microservicio de gestión y envío de comunicaciones: encargado de almacenar las comunicaciones que los inversores ven en su área privada y de enviar por mail aquellas comunicaciones que lo requieran. Cuenta con su propia db en MongoDB para controlar y gestionar los envíos. Recibe peticiones del API y reporta estado de sus operaciones a la misma.
- Microservicio de gestión documental: apoyándonos en la infraestructura S3 de Amazon, el servicio de gestión de documentos se encarga de almacenar y suministrar todo tipo de documentos a la plataforma. El acceso a cada documento está gestionado por el API y el microservicio solamente puede gestionar documentos (almacenar, servir o eliminar) a través de peticiones del API, que es quien controla los permisos. Cuenta con su propia base de datos mongoDB para la gestión interna de los archivos.
- Microservicio de pagos: se encarga de gestionar los pagos mensuales de intereses. Recibe solicitudes de pago desde la API y se encarga de comunicarse con Lemonway para ejecutar los pagos y monitorizar las colas de peticiones, los errores… Cuenta con su propia base de datos mongoDB para controlar el estado de cada uno de los pagos solicitados.
- Microservicio de notificaciones: encargado de enviar notificaciones por SMS para dar cobertura al sistema de OTP. Cuenta con su propia base de datos en mongoDB para controlar el proceso de validación de las claves por SMS.

b. asociadas al panel de administración de la misma

4. Procedimiento de comunicación de incidencias

4.1. Alertas derivadas de Monitorizaciones de servicios

a. Caída o degradación del nivel de respuesta de los servicios de infraestructura por ataque de Denegación de servicio; reportes:
    a. Alerta de caída por mail a la cuenta de soporte de Housers a través de sistema de monitorización externo. La comunicación se produce en el momento de la caída, es inmediata y automática.
    b. En el caso de la ralentización, comunicación por parte de usuarios de la plataforma o de los trabajadores de Housers. La comunicación se produce cuando un usuario detecta la bajada de rendimiento.
b. Fallo en la conectividad del API con LemnonWay; reportes:
    a. Alerta de fallo de conexión con LemonWay a través de email a cuenta de soporte de Housers enviado por el API. La comunicación se produce en el momento del corte, es inmediata y automática.
c. Bloqueo del sistema de BD; reportes:
    a. Alerta de fallo de conexión con DB a través de email a cuenta de soporte de Housers enviado por el API. La comunicación se produce en el momento del corte, es inmediata y automática.
d. Fallo en alguno de los microservicios alojados en el entono de Amazon WS; reportes:
    a. Alerta de fallo de conexión con microservicio a través de email a cuenta de soporte de Housers enviado por el API. La comunicación se produce en el momento del corte, es inmediata y automática.

4.2. Alertas derivadas de monitorizaciones de seguridad activa

e. Notificaciones del centro de alerta temprana; reportes:
    a. Envío de email de notificación de vulnerabilidad al correo de soporte de Housers. Envío automatizado e inmediato al detectar la caída.
f. Alertas derivadas de auditorías periódicas de seguridad; reportes:
    a. Envío de informe derivado de las auditorias de seguridad (semanales y trimestrales) al correo del CTO de Housers. Envío de informe semanalmente.

4.3. Alertas derivadas del error en funcionalidades del a plataforma

g. asociadas a la operativa de los inversores; reportes:
    a. Alerta de fallo a través de email a cuenta de soporte de Housers enviado por el API. La comunicación se produce en el momento del corte, es inmediata y automática.
    b. Aviso directo por mail / teléfono por parte de usuarios de Housers o trabajadores de Housers. La comunicación se produce cuando un usuario detecta el problema.
h. asociadas al panel de administración de la misma; reportes:
    a. Alerta de fallo a través de email a cuenta de soporte de Housers enviado por el API
    b. Aviso directo por mail / teléfono por parte de trabajadores de Housers. La comunicación se produce cuando un usuario detecta el problema.

5. Respuesta a las incidencias reportadas

El CTO es el responsable de garantizar la continuidad de las operaciones.

5.1. Tiempos de reacción:

Tipo de incidencia	gravedad	Tiempo de reacción
Consecuencia insignificante	1	24-48 h
Consecuencia aceptable	2	24-48 h
Consecuencia mayor	3	Reacción inmediata después de la comunicación
Consecuencia catastrófica	4	Reacción inmediata después de la comunicación

5.2. Respaldo de la información y sistemas de recuperación:

- Cluster de sistema de contenedores en servicios de infraestructura cloud redundados:
    - Al estar todo el sistema redundado, permite que el fallo en alguno de los nodos del cluster sea paliado por el resto de nodos, manteniendo la continuidad del servicio.
    - Las copias de seguridad se realizan en dos niveles:

        - Copia instantánea de cada instancia de servicio de cómputo, que permite la recuperación inmediata de un estado anterior de la misma instancia.
        - Copia de datos en otros servicios de cómputo cloud, dentro de la UE (2-4 horas de recuperación).
    - Los microservicios alojados en Amazon cuentan con todos los niveles de protección, backup y continuidad de negocio que Amazon es capaz de ofrecer.
- Backup de base de datos:
    - Instancia clonada, sincronizando en modo pasivo. Permite una rápida recuperación de los datos y sin pérdidas de información.
    - Copia instantánea de la base de datos cada 30 minutos. Historial de copias almacenadas: 14 días. Permite la recuperación rápida con una pérdida máxima de 30 minutos de información.
    - Copia diaria de la base de datos en un segundo proveedor cloud, dentro de la UE. Historial de copias almacenadas: 30 días. Permite recuperar los datos con una pérdida máxima de 30 minutos.

5.3. Información bancaria y documentación de usuarios

- Además de los sistemas de backup anteriormente descritos, toda la información de wallets e inversores se encuentra replicada en el sistema de Lemonway, que cuenta a su vez con sus propios sistemas de garantía de continuidad de negocio y copia de seguridad.

5.4. Procedimiento del proceso de respuesta:

- Identificación del evento desencadenador de la incidencia
- Análisis de alcance de la incidencia:
    - Identificación de servicios afectados.
    - Identificación de usuarios afectados: usuarios anónimos, inversores, administradores de la plataforma, …
    - Afectación de datos: tablas de datos, históricos, logs, …
    - Afectación temporal: identificación de problemas derivados de la incidencia anteriores a su detección.
    - Identificación de posibles vulnerabilidades del sistema.
- Análisis de la solución planteada:

- Análisis del checkpoint a partir del cual se plantea la solución: creación de nueva rama para un hotfix y backup de datos.
- Análisis del código desarrollado para solucionar el problema.
- Análisis de la relación de dicho código con el resto de servicios del sistema.
- Análisis de los datos resultantes.
- Análisis de la seguridad del sistema una vez aplicada la solución

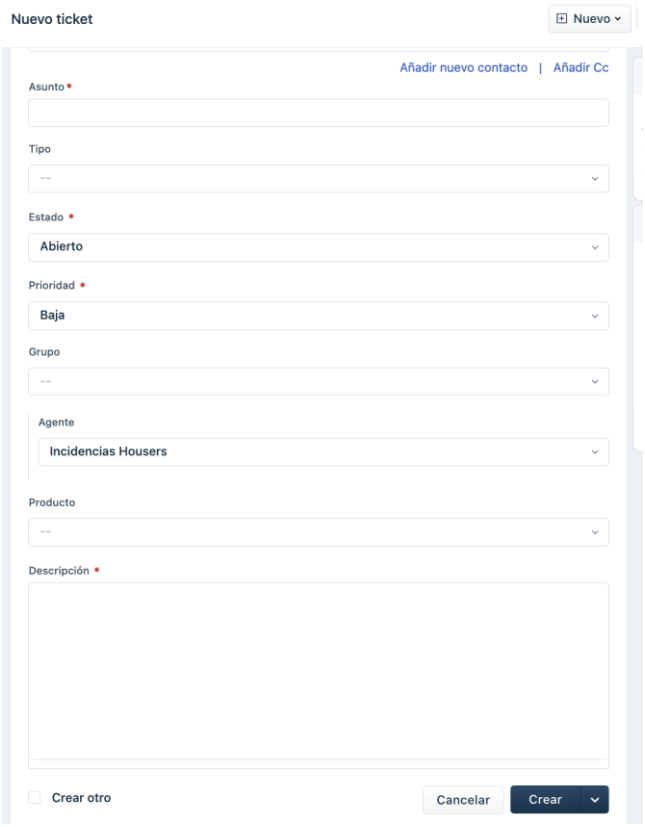
- Evaluación de la respuesta:
  - Propuesta de acciones a llevar a cabo para evitar que se repita la incidencia.
  - Propuesta de refactorización del servicio afectado en caso de ser necesario.
  - Análisis de tiempo y recursos dedicados a la resolución.
  - Evaluación del impacto sobre los diversos departamentos: Customer Care, Marketing, Real State, Financial, Legal, Institutional.
  - Evaluación del impacto sobre la relación empresa-cliente.
  - Evaluación del impacto sobre la confiabilidad de la empresa.
  - Desarrollo de un informe completo de la incidencia.

6. Seguimiento y archivo

Tenemos implantado un sistema de declaración y seguimiento de incidencias a través de Freshdesk. Este sistema permite la declaración, seguimiento y archivo de todas las incidencias declaradas para su posterior revisión.

Con posterioridad a la resolución de la incidencia, se analizan las causas y se concluyen las medidas preventivas o paliativas.

A continuación, se muestra el formulario de declaración de incidencia o ticket:



7. Periodicidad de las actualizaciones

Cada 3 meses se realiza una auditoria de seguridad y se aplican las medidas necesarias para evitar los riesgos.

Guía ESMA

Articulo 1

Definición

A los efectos del presente Reglamento, se aplicarán las siguientes definiciones:

a) «servicios críticos»: los servicios operativos y comerciales cuyo defecto o incumplimiento en su desempeño afectaría materialmente el cumplimiento continuo de un proveedor de servicios de crowdfunding con las condiciones y obligaciones de su autorización o sus otras obligaciones en virtud del Reglamento (UE) 2020/1503, o su rendimiento financiero, o la solidez o la continuidad de sus servicios y actividades de crowdfunding, en particular frente a sus clientes.

(b) 'fallo' significa cualquier procedimiento de insolvencia o pre-insolvencia aplicable bajo legislación nacional o cualquier interrupción significativa del negocio.

(c) "interrupción significativa del negocio" significa un defecto o incumplimiento significativo que materialmente perjudica el desempeño de los servicios críticos.

Artículo 2

Contenido mínimo del plan de continuidad del negocio

1. Los proveedores de servicios de financiación participativa desarrollarán un plan detallado de continuidad del negocio para abordar los riesgos asociados con su fracaso.

2. El plan de continuidad del negocio incluirá, entre otros:

a) medidas y procedimientos encaminados a garantizar la continuidad del suministro de servicios relacionados con inversiones existentes;

b) medidas y procedimientos encaminados a garantizar la buena administración de los acuerdos entre el proveedor de servicios de crowdfunding y sus clientes y la buena administración de datos comerciales críticos;

Artículo 3

Continuidad de la prestación de servicios críticos

1. El plan de continuidad del negocio garantizará que los servicios críticos, incluidos los subcontratados a terceros, se siguen realizando a pesar del fracaso del servicio de crowdfunding proveedor o el tercero al que se hayan subcontratado los servicios críticos.

2. Las medidas pertinentes se adaptarán al modelo de negocio del servicio de financiación participativa e incluirá disposiciones encaminadas a garantizar la continuidad de los servicios a través de la subcontratación de algunos o todos estos servicios críticos a una tercera entidad.

3. El plan de continuidad del negocio incluirá disposiciones para:

(a) notificación al cliente sobre la ocurrencia de un evento de falla

(b) el acceso de los clientes a la información relacionada con sus inversiones;

(c) en su caso, la continuación del servicio de los préstamos pendientes;

d) en su caso, la continuación de los servicios de pago a que se refiere el artículo 10 del Reglamento (UE) 2020/1503, incluidas las disposiciones a que se refiere el artículo 10, apartado 5 del mismo;

(e) en su caso, la entrega de los acuerdos de custodia de activos a que se refiere el Artículo 10 del Reglamento (UE) 2020/1503.

Artículo 4

Buena administración de los acuerdos

1. El plan de continuidad de las operaciones deberá, teniendo en cuenta la naturaleza, la escala y la complejidad del proveedor de servicios de crowdfunding, así como su modelo de negocio, detallar los pasos destinados a la buena administración de los acuerdos entre el proveedor de servicios de crowdfunding y su clientela.

2. Los trámites a que se refiere el apartado 1 se aplicarán a:

a) acuerdos entre el proveedor de servicios de financiación participativa y sus clientes, incluidos información que es de importancia crítica para la buena administración de los acuerdos,

b) los resultados de la prueba de conocimientos básicos a que se refiere el artículo 21 del Reglamento (UE) 2020/1503 y

(c) otros datos comerciales críticos.

3. Los trámites a que se refiere el apartado 1 consistirán, en su caso, en

a) el almacenamiento en un lugar seguro de los acuerdos a que se refiere el apartado 2, letra a), cuando originales sólo están disponibles en papel, y

(b) la copia de seguridad pertinente de los documentos y la información a que se refiere el apartado 2

4. Información y acuerdos que permitan rastrear los pagos realizados por los inversores y el proyecto propietarios se considerarán datos comerciales críticos a efectos de la letra c) del párrafo 2.

Artículo 5

Procedimientos

1. Los procedimientos a que se refiere el artículo 2, apartado 2, letras a) y b), se adaptarán a la

modelo de negocio del proveedor de servicios de financiación participativa e incluirá al menos:

(a) una compilación de una lista de detalles de contacto de las personas o departamentos a cargo en caso de incumplimiento del proveedor de servicios de crowdfunding;

(b) la identificación de, al menos, los tres escenarios más probables de falla y la descripción de las medidas a tomar para mitigar su impacto en la continuidad de los servicios críticos,

c) las disposiciones relativas al acceso del personal del proveedor de servicios de financiación participativa al espacio de trabajo y red de la empresa;

(d) disposiciones relativas al acceso a la información del cliente y, en su caso, a los activos del cliente;

e) una identificación de los riesgos operativos y financieros, así como medidas para reducir su ocurrencia;

(f) una identificación de los sistemas comerciales críticos y las medidas de contingencia para garantizar su continuidad

(g) una identificación de las relaciones comerciales críticas (incluidas las funciones subcontratadas);

h) procedimientos destinados a garantizar la continuidad de la comunicación entre los proveedor de servicios de crowdfunding, sus clientes, socios comerciales, empleados y autoridades competentes.