HOUSERS
SMART INVESTMENT

# Contenido

# 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.<br>• Análisis de la situación.<br>• Activación o no del plan de recuperación.<br>• Seguimiento del proceso de recuperación.<br>• Evaluación de los daños. | CTO (líder)<br>Responsable de sistemas |
| Equipo de Recuperación | Restablecer todos los servicios principales de TI que son: | CTO (líder) |

| | | |
|---|---|---|
| | • Servicio de base de datos MariaDB<br>• Servicio API<br>• Servicio web front<br>• Servicio web admin<br>• Servicio web blogs<br>• Microservicio de gestión de comunicaciones<br>• Microservicio de gestión documental<br>• Microservicio de pagos<br>• Microservicio de notificaciones<br>• Servidor de archivos oficina Housers | Responsable de sistemas (suplente)<br><br>Asistentes de Desarrollo de Software |
| Equipo de Pruebas | Realizarán las pruebas de verificación de operación de los servicios principales de TI.<br><br>Cada perfil debe tener su plan de pruebas de verificación el cual debe entregar al equipo de recuperación. | Responsable de Calidad de Software (CTO)<br><br>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 CTO 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]

[1] **Datos del ISP**: Amazon webservices (AWS) aloja los siguientes servicios:
• API
• MariaDB
• Web front
• Web admin

c. Fallo en la conectividad del API con LemnonWay
d. Bloqueo del sistema de BD

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
    b. asociadas al panel de administración de la misma

## 4. Procedimiento de comunicación de incidencias

### 4.1. Sistema de monitorización activa

- A través del sistema Teramonitor activado con el despliegue de la infraestructura en AWS, se realiza un seguimiento en tiempo real de todos los eventos relacionados tanto con el funcionamiento de la infraestructura como con el mantenimiento y backup de la misma.
- El servicio de monitorización se encuentra en el nodo de París de Amazon Web Services, mientras que los servicios de Pro están en Frankfurt y los de desarrollo en Irlanda.

### 4.2. Alertas derivadas de Monitorizaciones de servicios

a. Caída o ralentización del nivel de respuesta del servidor 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 (Uptimerobot). 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. No respuesta del servidor por caída de la conectividad del isp; reportes:
    a. Alerta de caída por mail a la cuenta de soporte de Housers a través de sistema de monitorización externo (Uptimerobot). La comunicación se produce en el momento de la caída, es inmediata y automática.
    b. Alerta por caída emitida por el departamento de sistemas externo (proporcionado por la empresa Teralevel) a partir de las alertas recibidas desde el sistema de monitorización Teramonitor. Esta alerta es emitida bien a través de correo electrónico o bien a través del canal de soporte específico que ambas empresas comparten en Microsoft Teams.
c. 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.
d. 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.
    b. Alerta por caída emitida por el departamento de sistemas externo (proporcionado por la empresa Teralevel) a partir de las alertas recibidas desde el sistema de monitorización Teramonitor. Esta alerta es emitida bien a través de correo electrónico o bien a través del canal de soporte específico que ambas empresas comparten en Microsoft Teams.

### 4.3. 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 al correo del CTO de Housers.

4.4. 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 a través del formulario de soporte de la web por parte de usuarios de Housers o a través del sistema externo de soporte (Freshdesk) comunicado por los 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 a través del sistema de soporte externo (Freshdesk) 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 servidores en entorno Cloud de Amazon Web Services:
    - Los servicios de producción están desplegados y distribuidos entre los 3 nodos de AWS localizados en Frankfurt. Por su parte, los servicios de backup y desarrollo se encuentran desplegados y distribuidos en los 3 nodos de AWS localizados en Irlanda. Finalmente, los servicios de monitorización y control están desplegados en los 3 nodos de AWS localizados en París. De esta forma se garantiza la integridad y la estabilidad de los servicios y ante una caída de uno de los nodos se puede recuperar el servicio en cualquier otro o incluso migrarlo a una de las otras 2 zonas.
    - Sistema de base de datos
        - La infraestructura cuenta con 2 entornos: uno de producción desplegado en Frankfurt y otro de desarrollo desplegado en Irlanda.
        - Cada uno de estos entornos cuenta con 2 cluster de base de datos: un cluster para MariaDB con 3 nodos y un cluster de MongoDB con otros 3 nodos.
- Backup de base de datos:

- Sincronización en tiempo real entre los nodos del cluster de base de datos. Este sistema previene la caída en alguno de los 3 nodos en que está implementado y permite funcionar incluso con solo 1 de los 3 nodos.
- Todos los días se realiza una copia completa de la base de datos. Una vez realizada la copia, ésta se monta en el servidor de base de datos de desarrollo, ubicado en el nodo de Irlanda de Amazon y se checkea la integridad del contenido. De forma adicional, el backup también se manda al sistema de almacenamiento de Amazon S3 (Nodo de Frankfurt) y a la NAS ubicada en las oficinas de Housers Madrid, con lo que se garantiza la continuidad de negocio ante cualquier contingencia.
- El sistema cuenta con un historial de copias diario ininterrumpido desde la implantación de la infraestructura en AWS.

### 5.3. Información bancaria y documentación de usuarios

- Los archivos transaccionales de la plataforma (documentación de clientes y proyectos) se encuentran almacenados en el servicio S3 de Amazon, que cuenta con todos los sistemas de protección ante pérdida de datos y seguridad de la información que un gigante como Amazon puede proporcionar. Dichos archivos están ubicados en el nodo de Frankfurt de S3, compuesto a su vez por 3 nodos, de forma que la caída en uno de ellos no afecte en nada ni a la persistencia ni al funcionamiento normal del sistema
- 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. Copia de seguridad del código fuente

- La copia de seguridad del código fuente de la plataforma se encuentra en dos capas: en un servicio Git local de cada desarrollador y en un servicio Git externo.

5.5. 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 evitar la repetición de 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 que la originaron y las posibles medidas preventivas a tomar, así como las posibles actualizaciones que se puedan derivar de estas conclusiones a integrar en el proceso de respuesta.

## 7. Periodicidad de las actualizaciones

El sistema de monitorización activa a través de Teramonitor permite detectar amenazas en tiempo real y aplicar las medidas necesarias para evitar riesgos y corregir vulnerabilidades.