HOUSERS
SMART INVESTMENT

Índice

POLÍTICA DE CONTINUIDADE DE NEGÓCIOS

1. Inrodução

O objectivo do Plano de Continuidade dos Serviços de TI é definir com precisão de que forma a HOUSERS irá recuperar ou continuar o funcionamento dos serviços, aplicações, sistemas ou componentes de TI ao nível acordado nos requisitos empresariais.

Este plano aplica-se a todas as actividades críticas no âmbito do Sistema de Gestão da Continuidade dos Serviços de TI.

Os usuários deste documento são todos os membros do pessoal, tanto interno como externo, que têm um papel na continuidade do serviço de TI.

2. Responsabilidade pela implementação da Política de continuidade de negócios

As equipas de trabalho, as suas actividades e os seus membros são conformados de acordo com a seguinte tabela::

Equipas	Funções	Integrantes
Equipa Director	Dirigir as actividades durante a contingência e recuperação. • Análise da situação. • Activação ou não do plano de recuperação. • Seguimento do processo de recuperação. • Avaliação de danos.	CTO (líder) Responsável de Sistemas
Equipa de Recuperação	Restaurar todos os serviços principais de TI que são: • Serviço de Base de Dados MariaDB • Serviço API • Serviço web front	CTO (líder) Responsável de Sistemas (suplente)

	• Serviço de administração web • Blogs serviço web • Micro-serviço de gestão de comunicações • Micro-serviço de gestão de documentos • Micro-serviço de pagamento • Micro-serviço de notificações • Servidor de arquivos do escritório da Housers	Assistentes de Desenvolvimento de Software
Equipa de Testes	Realizarão os testes de verificação operacional dos principais serviços informáticos. Cada perfil deve ter o seu plano de teste de verificação que deve ser entregue à equipa de recuperação.	Gestor de Qualidade de Software (CTO) Assistentes de Desenvolvimento de Software

3. Identificação de Incidentes

A avaliação do risco avalia o nível da ameaça (ou seja, incidente perturbador) e a medida em que a HOUSERS são vulneráveis a essa ameaça. A avaliação dos riscos é implementada através da Carta de Avaliação e Tratamento dos Riscos. O processo de avaliação de risco é coordenado pelo CTO e a avaliação de risco para serviços individuais é realizada pelos gestores de serviços.

3.1. Níveis de categorização de incidentes:de:

Consequência insignificante	1	A duração do incidente perturbador não afecta significativamente as finanças da organização, as obrigações legais ou contratuais, ou a reputação.
Consequência aceitável	2	A duração do incidente perturbador causa danos às finanças, obrigações legais ou contratuais ou à reputação da organização, mas esse dano é ainda aceitável tendo em conta a sua magnitude e circunstâncias específicas.
Consequência maior	3	A duração do incidente perturbador causa danos às finanças, obrigações legais ou contratuais ou à reputação da organização e que os danos não são aceitáveis devido à sua magnitude e circunstâncias específicas.
Consequência catastrófica	4	A duração do incidente perturbador causa danos importantes às finanças da organização, obrigações legais ou contratuais ou reputação que a levarão a perder a maior parte do seu capital e/ou a ter de encerrar definitivamente as suas operações.

3.2. Tipos de alertas

1. Alertas derivados do Monitorização de serviços:
    a. Queda ou desaceleração do nível de resposta do servidor devido a um ataque de negação de serviço.
    b. Nenhuma resposta do servidor devido a uma queda na conectividade do isp[1]

[1] **Dados do ISP**: Amazon webservices (AWS) hospeda os seguintes serviços:
• API
• MariaDB
• Web front
• Web admin

c. Falha de conectividade API com LemnonWay
d. Bloqueio do sistema BD

2. Alertas derivados do monitorização da segurança activa
    a. Notificações do centro de alerta precoce
    b. Alertas derivados de auditorias periódicas de segurança
3. Alertas derivados de erros nas funcionalidades da plataforma
    a. associado às operações do investidor
    b. associado ao painel de administração da plataforma

4. **Procedimento de comunicação de incidentes**

4.1. Sistema de monitorização activa

- Através do sistema Teramonitor activado com a implementação da infra-estrutura no AWS, todos os eventos relacionados tanto com o funcionamento da infra-estrutura como com a sua manutenção e backup são monitorizados em tempo real.
- O serviço de monitorização está localizado no nó parisiense de Amazon Web Services, enquanto os serviços Pro estão em Frankfurt e os serviços de desenvolvimento estão na Irlanda.

4.2. Alertas derivados dos serviços de Monitorização

a. Queda ou desaceleração do nível de resposta do servidor devido a ataque de Negação de Serviço; relatórios:
    a. Alerta de inactividade por e-mail para a conta de apoio Housers através de um sistema de monitorização externo (Uptimerobot). A comunicação ocorre no momento da queda, é imediata e automática.
    b. Em caso de abrandamento, a comunicação pelos usuários da plataforma ou funcionários da Housers. A comunicação ocorre quando um usuário detecta a queda de desempenho.

b. Nenhuma resposta do servidor devido a uma queda na conectividade do isp; relatórios:
    a. Alerta de inactividade por e-mail para a conta de apoio Housers através de um sistema de monitorização externo (Uptimerobot). A comunicação ocorre no momento da queda, é imediata e automática.
    b. Alerta de inactividade emitido pelo departamento de sistemas externos (fornecido pela empresa Teralevel) a partir dos alertas recebidos do sistema de monitorização Teramonitor. Este alerta é emitido por correio electrónico ou através do canal de apoio específico que ambas as empresas partilham em Microsoft Teams.
c. Falha na conectividade do API com a LemnonWay; relatórios:
    a. Alerta de falha de ligação com a LemonWay através de e-mail para a conta de suporte Housers enviada pela API. A comunicação ocorre no momento do corte, é imediata e automática.
d. Bloqueio do sistema DB; relatórios:
    a. Alerta de falha de ligação DB via e-mail à conta de suporte Housers enviada pela API. A comunicação ocorre no momento do corte, é imediata e automática.
    b. Alerta de inactividade emitido pelo departamento de sistemas externos (fornecido pela empresa Teralevel) a partir dos alertas recebidos do sistema de monitorização Teramonitor. Este alerta é emitido por correio electrónico ou através do canal de apoio específico que ambas as empresas partilham em Microsoft Teams.

4.3. Alertas derivados da monitorização da segurança activa

e. Notificações do centro de alerta precoce; relatórios:

a. O envio de notificação por e-mail de vulnerabilidade para o Housers suporta e-mail. Envio automatizado e imediato após a detecção da queda.

f. Alertas derivados de auditorias periódicas de segurança; relatórios:

a. Envio do relatório derivado das auditorias de segurança para o e-mail do CTO da Housers.

4.4. Alertas derivados do erro nas funcionalidades da plataforma.

g. associados ao funcionamento dos investidores; relatórios:

a. Alerta de falha via e-mail para a conta de suporte Housers enviada pela API. A comunicação ocorre no momento da interrupção, é imediata e automática.

b. Notificação directa através do formulário de apoio web pelos usuários da Housers ou através do sistema de apoio externo (Freshdesk) comunicado pelos funcionários da Housers. A comunicação ocorre quando um usuário detecta o problema.

h. associado ao painel de administração do mesmo; relatórios:

a. Alerta de falha via e-mail para a conta de suporte Housers enviada pela API.

b. Aviso directo através do sistema de apoio externo (Freshdesk) pelos trabalhadores da Housers. A comunicação ocorre quando um usuário detecta o problema.

5. **Resposta aos incidentes comunicados**

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

5.1. Tempos de resposta:

Tipo de incidência	**gravidade**	**Tempo de resposta**
Consequência insignificante	1	24-48 h.

Consequência aceitável	2	24-48 h
Consequências maior	3	Reacção imediata após a comunicação
Consequência catastrófica	4	Reacção imediata após a comunicação

5.2. Sistemas de backup e recuperação de informação:

- Cluster de servidores no ambiente Amazon Web Services Cloud:
  - Os serviços de produção são implantados e distribuídos entre os 3 nós AWS localizados em Frankfurt. Por outro lado, os serviços de apoio e desenvolvimento são implantados e distribuídos nos 3 nós AWS localizados na Irlanda. Finalmente, os serviços de monitorização e controlo são implantados nos 3 nós AWS localizados em Paris. Desta forma, a integridade e estabilidade dos serviços é garantida e, em caso de queda de um dos nós, o serviço pode ser recuperado em qualquer outro nó ou mesmo migrado para uma das outras 2 zonas.
    - Sistema de base de dados
      - A infra-estrutura tem 2 ambientes: um ambiente de produção implantado em Frankfurt e um ambiente de desenvolvimento implantado na Irlanda.
      - Cada um destes ambientes tem 2 clusters de bases de dados: um cluster MariaDB com 3 nós e um cluster MongoDB com outros 3 nós.
- Backup da base de dados:
  - Sincronização em tempo real entre os nós do cluster da base de dados. Este sistema evita a queda em qualquer um dos 3 nós em que é implementado e permite trabalhar mesmo com apenas 1 dos 3 nós.
  - Todos os dias é realizada uma cópia completa da base de dados. Uma vez realizada a cópia, esta é montada no servidor da base de dados de desenvolvimento, localizado no nó da Amazon Ireland e a integridade

do conteúdo é verificada. Além disso, o backup é também enviado para o sistema de armazenamento Amazon S3 (Nó de Frankfurt) e para o NAS localizado nos escritórios de Housers Madrid, que garante a continuidade do negócio em caso de qualquer contingência.

- O sistema tem um historial de cópias diárias ininterruptas desde a implementação da infra-estrutura na AWS.

5.3. Informação bancária e documentação dos usuários

- Os ficheiros transaccionais da plataforma (documentação do cliente e do projecto) são armazenados no serviço S3 da Amazon, que possui todos os sistemas de protecção de perda de dados e de segurança da informação que um gigante como a Amazon pode fornecer. Estes ficheiros estão localizados no nó de Frankfurt de S3, que por sua vez consiste em 3 nós, de modo a que a queda num deles não afecte a persistência ou o funcionamento normal do sistema.
- Para além dos sistemas de backup acima descritos, todas as informações sobre carteira e investidores são replicadas no sistema Lemonway, que por sua vez tem os seus próprios sistemas de continuidade de negócio e de garantia de backup.

5.4. Cópia de segurança do código fonte

- A cópia de segurança do código fonte da plataforma está em duas capas: num serviço Git local de cada desenvolvedor e num serviço Git externo.

5.5. Procedimento do processo de resposta:

- Identificação do evento que desencadeia o problema.
- Análise do âmbito do incidente:
  - Identificação dos serviços afectados.
  - Identificação dos usuários afectados: usuários anónimos, investidores, administradores da plataforma, ...

- Impacto de dados: tabelas de dados, dados históricos, registos, …
- Impacto temporal: identificação de problemas derivados do incidente antes da sua detecção.
- Identificação de possíveis vulnerabilidades do sistema.

- Análise da solução proposta:
  - Análise do ponto de controlo a partir do qual a solução é proposta: criação de um novo ramo para um hotfix e backup de datos.
  - Análise do código desenvolvido para resolver o problema.
  - Análise da relação deste código com o resto dos serviços do sistema.
  - Análise dos dados resultantes.
  - Análise da segurança do sistema uma vez que a solução tenha sido aplicada.
- Avaliação da resposta:
  - Proposta de acções a levar a cabo para evitar a repetição da incidência.
  - Proposta de refactorização do serviço afectado, se necessário.
  - Análise do tempo e dos recursos dedicados à resolução.
  - Avaliação do impacto nos diferentes departamentos:Customer Care, Marketing, Real State, Financial, Legal, Institutional.
  - Avaliação do impacto sobre a relação empresa-cliente.
  - Avaliação do impacto sobre a fiabilidade da empresa.
  - Elaboração de um relatório completo do incidente.

6. Rastreio e arquivo

Implementámos um sistema de declaração e monitorização de incidentes através da Freshdesk. Este sistema permite a declaração, monitorização e arquivamento de todos os incidentes declarados para posterior revisão.

Após a resolução do incidente, são analisadas as causas que o originaram e as possíveis medidas preventivas a tomar, bem como as possíveis actualizações que podem ser derivadas destas conclusões para serem integradas no processo de resposta.

7. Periodicidade das actualizações

O sistema de monitorização activa através do Teramonitor permite-nos detectar ameaças em tempo real e aplicar as medidas necessárias para evitar riscos e corrigir vulnerabilidades.