**Universidade São Judas Tadeu**

Eduardo Cecilio Alves Santos – RA:824224719

Ian Bastos Leme de Moraes – RA:825111187

Kauan Camargo – RA: 825141414

Lucas Tosta Piola – RA:825137169

Victor Gonçalves Volpi – RA:825117218

Wagner Quispe Espinal – RA:823154959

# Sistemas Computacionais e Segurança

# (SCC)

São Paulo

2025

# Introdução da empresa e seu cenário

## Infraestrutura de TI

Servidores de Desenvolvimento (armazenamento de código-fonte, builds e assets de jogos)

Serviços de Backup (nuvem e local)

Servidores de Versionamento de Código (por exemplo, GitLab, GitHub Enterprise, Bitbucket)

Ambientes de Build e Teste Automatizado (Continuous Integration / Continuous Delivery - CI/CD)

## Plataformas de Desenvolvimento

Game Engines (Unity, Unreal Engine, Godot, etc.)

Frameworks de Desenvolvimento (para mobile, VR/AR, consoles)

Ferramentas de Modelagem e Animação 3D (Blender, Autodesk Maya, 3ds Max)

Softwares de Edição de Áudio (Audacity, FMOD, Wwise)

## Recursos Humanos

Desenvolvedores de Software (programadores de jogos, back-end, front-end)

Designers de Jogos (game designers, level designers)

Artistas Digitais (2D, 3D, animação)

Especialistas em Áudio (composição, efeitos sonoros)

Testadores (QA - Quality Assurance)

## Dados e Propriedade Intelectual

Código-fonte dos jogos

Assets (gráficos, animações, músicas, efeitos sonoros)

Documentos de Design de Jogos (GDD - Game Design Document)

Dados de Usuário (para jogos online ou com perfis de jogadores)

Contratos e Direitos Autorais

## Comunicação e Colaboração

Plataformas de Comunicação Interna (Slack, Microsoft Teams, Discord)

Gerenciamento de Projetos (Jira, Trello, Asana)

Sistemas de Repositório de Documentação (Confluence, Notion)

## Serviços de Distribuição e Marketing

Plataformas de Publicação de Jogos (Steam, Epic Games Store, PlayStation Network, Xbox Live, App Store, Google Play)

Serviços de Marketing e Relacionamento com a Comunidade (Redes Sociais, Discord Servers Oficiais, campanhas de mídia)

## Segurança da Informação

Sistemas de Autenticação e Controle de Acesso (VPNs, autenticação multifator, controle de identidade)

Ferramentas de Monitoramento de Segurança (SIEM, antivírus, firewalls)

Políticas de Backup e Recuperação de Desastres

# Recursos críticos identificados

## Infraestrutura de TI

Servidores de Versionamento de Código: fundamentais para colaboração e integridade do desenvolvimento.

Serviços de Backup (nuvem e local): essenciais para prevenção contra perda de dados.

Ambientes de Build e Teste Automatizado (CI/CD): garantem agilidade e qualidade nas entregas.

## Plataformas de Desenvolvimento

Game Engines (Unity, Unreal, etc.): pilares centrais na produção dos jogos.

Ferramentas de Modelagem e Animação 3D: indispensáveis para criação de conteúdo visual.

Frameworks de Desenvolvimento para plataformas específicas (VR, consoles, mobile): garantem compatibilidade com os dispositivos-alvo.

## Recursos Humanos

Desenvolvedores de Software: sem eles, o desenvolvimento para.

Designers de Jogos e Artistas Digitais: contribuem com o conteúdo criativo essencial.

Testadores (QA): críticos para garantir qualidade e funcionalidade dos jogos antes do lançamento.

## Dados e Propriedade Intelectual

Código-fonte dos jogos: base do produto e altamente sensível.

Assets (gráficos, som, animações): compõem o conteúdo final do jogo.

Documentos de Design (GDDs): guiam todo o processo de desenvolvimento.

Dados de Usuário: especialmente críticos em jogos online — implicações legais e operacionais.

## Comunicação e Colaboração

Plataformas de Comunicação Interna (Slack, Teams): essenciais para alinhamento de equipes.

Gerenciamento de Projetos (Jira, Trello): sem eles, pode haver perda de controle de cronogramas e tarefas.

## Serviços de Distribuição e Marketing

Plataformas de Publicação (Steam, App Store, etc.): canais de receita — sem acesso, não há vendas.

Serviços de Relacionamento com a Comunidade: importantes para suporte, feedback e marketing.

## Segurança da Informação

Sistemas de Autenticação e Controle de Acesso: protegem propriedade intelectual e dados sensíveis.

Políticas de Backup e Recuperação de Desastres: chave para continuidade em caso de falhas.

# Análise de continuidade – Ativos e riscos

## Infraestrutura de TI

| Ativo | Função | Impacto | RTO | RPO | Observações |
|---|---|---|---|---|---|
| Servidores de Desenvolvimento | Código e assets | Paralisa desenvolvimento | 4h | 1h | Prioridade alta |
| Backup (Nuvem e Local) | Proteção de dados | Perda de dados críticos | 8h | 24h | Redundância necessária |
| Versionamento (GitLab, etc.) | Controle de código | Perda de alterações | 2h | 30min | Fundamental |

## Plataformas de Desenvolvimento

| Ativo | Função | Impacto | RTO | RPO | Observações |
|---|---|---|---|---|---|
| Game Engines (Unity, Unreal) | Desenvolvimento | Desenvolvimento parado | 4h | 1h | Instalações alternativas |
| Modelagem 3D | Artes e animações | Área artística parada | 6h | 2h | Backup de arquivos |
| Edição de Áudio | Sons e trilhas | Entrega incompleta | 8h | 4h | Usar alternativas |

## Recursos Humanos

| Ativo | Função | Impacto | RTO | RPO | Observações |
|---|---|---|---|---|---|
| Desenvolvedores | Programação | Atraso e bugs | 1 dia | 1 dia | Ter plano de substituição |
| Designers | Mecânicas e níveis | Falha no design | 2 dias | 1 dia | Documentar bem |
| Artistas | Visuais 2D/3D | Atraso de assets | 2 dias | 1 dia | Acesso remoto |
| Especialistas de Áudio | Trilha sonora | Entregas incompletas | 3 dias | 2 dias | Priorizar trilhas principais |
| Testadores (QA) | Testes de qualidade | Bugs graves | 1 dia | 1 dia | Impacta reputação |

## Dados e Propriedade Intelectual

| Ativo | Função | Impacto | RTO | RPO | Observações |
|---|---|---|---|---|---|
| Código-fonte | Produto principal | Perda total | 1h | 0h | Backup constante |
| Assets | Gráficos e sons | Atrasos | 2h | 1h | Versionamento |
| GDD (Design Document) | Direcionamento | Confusão entre equipes | 4h | 2h | Controle rigoroso |
| Dados de Usuário | Perfis de jogadores | Perda de confiança | 2h | 30min | Criptografar |
| Contratos | Proteção legal | Multas, processos | 24h | 1 dia | Guardar cópias |

## Comunicação e Colaboração

| Ativo | Função | Impacto | RTO | RPO | Observações |
|---|---|---|---|---|---|
| Comunicação Interna | Comunicação rápida | Falha no time | 2h | 1h | Alternativas emergenciais |
| Gerenciamento de Projetos | Organização | Desorganização | 4h | 2h | Backups semanais |
| Documentação | Manual e GDD | Perda de referência | 6h | 2h | Exportação periódica |

## Distruibuição e Marketing

| Ativo | Função | Impacto | RTO | RPO | Observações |
|---|---|---|---|---|---|
| Publicação | Venda dos jogos | Perda de receita | 2h | 30min | Monitorar plataformas |
| Marketing | Divulgação e engajamento | Perda de comunidade | 6h | 4h | Agendamento prévio |

## Segurança de Informação

| Ativo | Função | Impacto | RTO | RPO | Observações |
|---|---|---|---|---|---|
| Autenticação e Acesso | Controle de usuários | Invasões | 1h | 0h | MFA obrigatório |
| Monitoramento | Alertas de ataques | Falhas na segurança | 1h | 30min | SIEM ativo |
| Backup e Recuperação | Recuperação de falhas | Perda de operação | 4h | 1h | Testar planos |

| Categoria | Recursos Críticos | Estratégias de Recuperação |
|---|---|---|
| | Servidores de Versionamento | Espelhamento de Dados, backups a cada 15 minutos, failover automático. |
| **TI/ Infraestrutura** | Backups em nuvem/local | Agendamentos automáticos e testes mensais de restauração. |
| | Ambientes (CI/CD) | Imagens Docker e scripts de provisionamento para restauração rápida. |
| **Plataformas de Desenvolvimento** | Game Engines (Unity, Unreal) | Licenças na nuvem, instalação automatizada via scripts. |
| | Ferramentas 3D e frameworks | Backup das versões utilizadas + documentação técnica para reinstalação. |
| **Recursos Humanos** | Desenvolvedores e artistas | Lista de substitutos/freelancers, documentação de onboarding, possibilidade de trabalho remoto. |
| | QA e testadores | Redistribuição de tarefas para outras equipes, testes automatizados como suporte. |
| | Código-fonte | Backup contínuo (versionamento). |
| **Dados e Propriedade Intelectual** | Assets (gráficos, áudio, etc.) | Backup diário automatizado + armazenamento redundante. |
| | GDDs e Documentação | Armazenamento em nuvem com versionamento ativado |
| | Dados do Usuário | Criptografia, backup contínuo em banco de dados, replicação |

| | | |
|---|---|---|
| **Comunicação e Colaboração** | Slack, Teams, Jira, Trello | Acesso via navegador em dispositivos alternativos, opção de canal alternativo para emergências. |
| **Distribuição e Marketing** | Steam, App Store | Documentação de credenciais e acesso de emergência, múltiplos admins |
| | Canais de Suporte / Comunicação | Equipe reserva com acesso aos canais, uso de redes sociais |
| | Autenticação e Acesso | Backup de configurações e logs, ferramenta SSO redundante |
| **Segurança da Informação** | Políticas de backup / DR | Procedimentos documentados, testes semestrais |
| | Monitoramento de Segurança | backups regulares dos logs de segurança. Adotar serviços de segurança baseados em nuvem. |

# Teste do Plano de Ação

## Ações Preventivas:

**Backups Diários Automatizados:**
Configurar rotinas de backup local e em nuvem para código-fonte, assets, dados de usuários e GDDs, com testes de restauração semanais.

**Redundância de Servidores:**
Utilizar servidores espelhados (on-premises e cloud) para ambientes de CI/CD, versionamento e serviços de build.

**Contratos de Suporte Prioritário:**
Firmar acordos com fornecedores de plataformas críticas (Unity, AWS, Slack, etc.) para atendimento rápido em emergências.

**Documentação e Treinamento:**
Manter planos atualizados e realizar treinamentos semestrais com os colaboradores para atuação em situações de crise.

## Ações em Caso de Interrupção:

**Ativação do Comitê de Continuidade:**
Grupo formado por líderes de TI, desenvolvimento e operações será imediatamente acionado.

**Avaliação Inicial e Isolamento:**
Identificar a natureza do incidente (falha técnica, ataque cibernético, desastre natural, etc.) e isolar sistemas afetados para conter danos.

**Comunicação Interna Rápida:**
Utilizar canais alternativos (e-mail pessoal, grupos de emergência no WhatsApp) caso Slack/Teams estejam fora do ar.

## Recuperação dos Recursos Críticos

**Restabelecimento de Servidores de Código e CI/CD:**
Prioridade máxima para retomar o desenvolvimento e integração contínua.

**Recuperação de Acessos às Plataformas de Comunicação e Gerenciamento:**
Necessárias para alinhar equipes e replanejar cronogramas.

**Restauração de Dados e Assets:**
Utilizar backups para restaurar os arquivos e dados mais recentes.

**Verificação de Integridade:**
Validar código e assets restaurados por meio de testes automatizados e QA.

## Continuidade Temporária

**Home Office com VPN Segura:**
Caso o escritório físico esteja inacessível, garantir operação remota com políticas de segurança.

**Infraestrutura Alternativa na Nuvem:**
Caso servidores locais falhem, migrar temporariamente ambientes para cloud (AWS, Azure, GCP).

**Equipes de Suporte Cross-Training:**
Desenvolvedores e designers terão treinamentos cruzados para cobrir funções essenciais em casos de ausência.

## Retorno à Normalidade

**Auditoria e Relatório Final:**
Documentar o ocorrido, medidas tomadas e impactos para aprendizado.

**Atualização do Plano:**
Revisar o Plano de Continuidade com base nas lições aprendidas.

**Apoio aos Colaboradores:**
Disponibilizar suporte emocional e psicológico em casos de crises intensas.

# Simulação de Crise Multicamadas

Sugere-se a realização de uma simulação semestral de cenário de crise, abrangendo múltiplas camadas de incidentes (ex: falha de servidor local, interrupção de serviço em nuvem e ataque cibernético simultâneo). Durante a simulação, o Comitê de Continuidade deverá ser acionado e seguir todos os protocolos descritos nas etapas do plano (resposta, recuperação, continuidade temporária e retorno à normalidade).

A simulação inclui:

Testes reais de restauração de backups em ambiente de homologação;

Uso de canais alternativos de comunicação (WhatsApp, e-mails pessoais);

Migração simulada de serviços locais para a nuvem;

Avaliação do tempo de resposta de cada equipe;

- Aplicação de formulário pós-simulação para coleta de feedback dos envolvidos;
- Emissão de relatório final com pontos fortes e oportunidades de melhoria.