Plano de Contingência Tecnológico

Documento Auvo Tecnologia S.A.

Sumário

1. Objetivo

O objetivo do plano é estabelecer procedimentos de mobilização e comunicação para controle e tratamentos de incidentes, com foco na redução de impacto negativo causado por desastres e no restabelecimento dos serviços prestados. Em caso de contingências e emergências que possam ocorrer durante as atividades na execução dos serviços de Tecnologia da Informação, o plano de contingência contém os procedimentos de correção e/ou eliminação dos problemas. Para tanto, esse plano deve assegurar que os processos críticos têm seus riscos identificados, avaliados, monitorados e controlados.

2. Aplicação

Este documento se aplica a todos os serviços e infraestruturas de Tecnologia da Informação sob responsabilidade da Auvo Tecnologia. Este documento deverá ser empregado no preenchimento dos planos de ações cabíveis à cada ocorrência.

3. Grupo Gestor de Crise

Cabe ao grupo identificar e analisar os impactos nos processos e perdas potenciais para garantir a continuidade dos serviços priorizando processos críticos por meio do estabelecimento de procedimentos, divisão de responsabilidades e alocação de recursos.

3.1 Equipe da Auvo Tecnologia

O Grupo Gestor de Crise será constituído pelos seguintes membros:

a) Diretor Geral;
b) Gerente de desenvolvimento;
c) Arquiteto de software;
d) Responsável pelo Setor de Infraestrutura.

3.2 Prestação de Serviços Terceirizados e Fornecedores

Se necessário, fabricantes e prestadores de serviços terceirizados serão acionados quando houver contrato de suporte e garantia vigentes, como nos casos do outsourcing de impressão e nos ativos de rede com garantia extendida ou vitalícia.

4. Atribuições do Grupo Gestor de Crise

a) Identificar e avaliar as principais situações de emergência;

b) Mensurar e gerenciar riscos, monitorar pontos frágeis, tangíveis e intangíveis e criar regras, procedimentos e controle;

c) Avaliar o custo de cada risco depois de multiplicá-los pela probabilidade de ocorrência desses riscos;

d) Assegurar o funcionamento dos serviços essenciais so serviço em situações de emergência, como inoperância de servidores, equipamentos e de conectividade, de banco de dados;

e) Determinar quais são as partes da estrutura da instituição são essenciais e não podem parar;

f) Desenvolver uma política de segurança e um ciclo de tratamento de risco na qual envolve a identificação dos ativos, as vulnerabilidades destes ativos, quais os riscos identificados e quais os riscos que serão de fato tratados;

g) Prever ou analisar o problema/fato ocorrido, definindo estratégia(s), metas, e ações a serem adotadas que durem até o retorno à situação normal de funcionamento da Instituição;

h) Propor procedimentos, controles e regras que possibilitem a ininterrupção das intervenções;

i) ter sempre um segundo plano para cada procedimento de crise;

j) acompanhar e orientar os relatórios das equipes envolvidas nos processos.

5. Avaliação, Aplicação e Melhoria Contínua do Plano

O Grupo Gestor de Crise ordinariamente reunir-se-á uma vez por semestre, e, extraordinariamente, em caso de evento significativo, a fim de analisar os planos e os cenários adversos que poderão influenciar a instituição.

6. Principais Riscos

O Plano de Contingência foi desenvolvido para ser acionado quando da ocorrência de cenários que apresentam risco à continuidade dos serviços essenciais. O quadro abaixo define estes riscos e aponta quais parâmetros para reportar as possíveis causas da ocorrência.

Evento	
01 Ataque Cibernético	Ataque virtual que comprometa o desempenho, os dados ou a configuração dos serviços essenciais
02 Indisponibilidade do banco de dados	Banco de dados corrompido, removido ou indisponível por tempo indeterminado
03 Falha em servidores de aplicação	Servidor corrompido, indisponível por tempo indeterminado ou removido

7. Estratégias de Controle, Monitoramento e Tratamento de Incidentes

7.1 Incidentes de Segurança e Ataques Cibernéticos

a) Caso sejam detectadas anomalias de tráfego de rede pela central de tratamentos de ameaça o tráfego deve ser monitorado, se necessário, origem e destino podem ser colocados em quarentena ou banidos da rede;

b) Salvar relatórios e logs de acesso para investigação futura.

7.2 Incidentes de Segurança e Ataques Cibernéticos

a) Caso o banco de dados fique indisponível o backup na nuvem primária será disponibilizado manualmente para uso das aplicações e restabelecimento do serviço;

b) Caso o backup primário apresenta falha, o backup da região secundária será utilizado para criação de um novo servidor de banco e dados;

c) Caso o último backup disponível não possua todos os dados, os aplicativos podem ser utilizados como fonte de dados para serem coletadas informações de serviços executados através dos aparelhos.

7.3 Falha em Servidores de Aplicação

a) Caso haja falha no servidor de aplicação causando indisponibilidade do mesmo o back up da máquina será acionado para responder às requisições;

b) Caso o backup do servidor apresentar falhas, um novo servidor pode ser configurado a partir da imagem de máquina armazenada na nuvem.

8. Política de Segurança

a) **Política e procedimentos para backup:** O backup dos servidores e sistemas é feito usando dois datacenters de nuvem diferentes como armazenamento seguro. Os Backups são realizados utilizando um software de backup dedicado apropriado para o sistema operacional utilizado;

b) **Status do backup:** O software de backup é configurado para alertar automaticamente o administrador para o status de qualquer backup realizado. O status do backup é analisado em uma base diária e quaisquer falhas identificadas são corrigidas;

c) **Ciclos de backup:**
Repositório de Dados - O backup completo dos sistemas importantes é realizado diariamente.

Esquema de rotação - É utilizado o método simples de rotação diária, sendo que, no mínimo, 15 (quinze) backups são mantidos.
São feitos backups:

- Diários, com retenção de 15 dias;
- Mensais com retenção de 1 ano;
- Anuais com retenção de 5 anos.

d) **Tempo de acesso logado em cada aplicação**

Auvo:

- **Plataforma Web:**
  Após logado o usuário perde login automaticamente após 8 horas, isso acontece independentemente de uso ou não do sistema durante essas 8 horas.

- **Aplicativo mobile:**
  Após logar o usuário não é deslogado automaticamente, as duas opções para deslogar o usuário são via ação no aplicativo ou ao forçar a desconexão via aplicação web.

AuvoDesk:

- Após logado o usuário perde login automaticamente após 14 dias, isso acontece independentemente de uso ou não do sistema durante esses 14 dias.

- Ao fazer login caso a opção "Permanecer conectado" seja escolhida, o tempo de desconexão automática é extendido em 14 dias sempre que o usuário interagir com o sistema.

Central do cliente:

- Após logado o usuário perde login automaticamente após 14 dias, isso acontece independentemente de uso ou não do sistema durante esses 14 dias.

- Ao fazer login caso a opção "Permanecer conectado" seja escolhida, o tempo de desconexão automática é estendido em 14 dias sempre que o usuário interagir com o sistema.

9. Versionamento

Para garantir a compatibilidade, manutenção e evolução contínua de nossas plataformas, adotamos um sistema de versionamento semântico estruturado. Esse sistema organiza as versões de cada aplicação, de forma a facilitar o controle de atualizações e minimizar possíveis incompatibilidades.

O versionamento semântico das aplicações Auvo, AuvoDesk, Central do cliente e do aplicativo mobile Auvo segue o padrão X.Y.Z, onde cada número indica o tipo de mudança realizada:

- **X (versão major):** Incrementado em mudanças que causam incompatibilidades com versões anteriores da API;
- **Y (versão minor):** Incrementado para novas funcionalidades que mantêm a compatibilidade com versões anteriores;
- **Z (versão patch):** Incrementado para correções de bugs que não afetam a compatibilidade.

Para a API pública de integração, utilizamos um sistema de versionamento simplificado com um único número de versão, alterado apenas para mudanças que causam incompatibilidades. Essa abordagem permite comunicar de forma clara e direta a estabilidade e as mudanças na API, facilitando o planejamento de integrações por parte de clientes e parceiros.

O uso consistente desse sistema de versionamento, integrado a um plano robusto de contingência e backup, permite gerenciar e restaurar versões específicas de forma rápida e segura, assegurando a continuidade do serviço e a confiabilidade das integrações.

Análise crítica

Elaborador	Revisor	Aprovador
Nome: Maicon Alves	Nome: Valmir Caixeta	Nome: Marcio Alves
Função: Líder técnico	Função: Diretor de TI	Função: Responsável técnico
ASS: Assinado por: Maicon Araujo 746D597B6D5C4E9...	ASS: Assinado por: Valmir Vieira 363796EA80BF41F...	ASS: Assinado por: 491498C104C843D...
Data: 04/12/2024	Data: 04/12/2024	Data:: 04/12/2024

Alterações desta revisão

Revisão	Data	Descrição da alteração / Motivo
00	19/04/2023	Emissão inicial
01	04/11/2024	Adição do versionamento semântico das aplicações
02	04/12/2024	Adicionada a documentação do tempo de acesso logado em cada aplicação

comercial@auvo.com.br
0800 000 0662
auvo.com
@auvotecnologia
/auvotechnology
/company/auvo-tecnologia/