

[logotipo da organização]

[nome da organização]

Commented [AES1]: Todos os campos desde documento que aparecem entre colchetes devem ser preenchidos.

PLANO DE RECUPERAÇÃO DE DESASTRE

Commented [AES2]: Para aprender mais sobre planos de recuperação de desastre, leia este artigo:

Recuperação em caso de desastre vs. continuidade de negócios
<https://advisera.com/27001academy/pt-br/blog/2010/12/29/recuperacao-em-caso-de-desastre-vs-continuidade-de-negocios/>

Commented [AES3]: O sistema de codificação do documento deve estar de acordo com o atual sistema de codificação de documentos da organização. Caso não haja um sistema desse tipo na organização, esta linha pode ser excluída.

Código:	
Versão:	
Data da versão:	
Criado por:	
Aprovado por:	
Nível de confidencialidade:	

Histórico de alterações

Data	Versão	Criado por	Descrição da alteração
	0.1	Advisera	Esboço básico do documento

Sumário

1. FINALIDADE, ESCOPO E USUÁRIOS	3
2. REFERENCE DOCUMENTS	3
3. PREMISSAS / LIMITAÇÕES	3
4. INFORMAÇÕES GERAIS	3
5. PAPÉIS E INFORMAÇÕES DE CONTATO.....	4
6. AUTORIZAÇÃO EM UMA CRISE	5
7. EVITANDO UM PONTO ÚNICO DE FALHA	5
8. RECURSOS NECESSÁRIOS	6
9. ETAPAS DE RECUPERAÇÃO PARA A INFRAESTRUTURA DE TI / SERVIÇOS DE TI.....	8
10. MANUTENÇÃO E REVISÃO DESTE PLANO	8
11. GESTÃO DE REGISTROS MANTIDOS DE ACORDO COM ESTE DOCUMENTO.....	9
12. VALIDADE E GESTÃO DE DOCUMENTOS.....	9
13. DOCUMENTOS ADICIONAIS.....	10

1. Finalidade, escopo e usuários

A finalidade do Plano de recuperação de desastre é definir precisamente como a [nome da organização] irá recuperar sua infraestrutura de TI e serviços de TI dentro dos prazos estabelecidos no caso de um desastre ou outro incidente disruptivo. O objetivo deste Plano é completar a recuperação da infraestrutura de TI e serviços de TI dentro do objetivo de tempo de recuperação estabelecido (recovery time objective – RTO) e do objetivo de ponto de recuperação (recovery point objective – RPO).

Este Plano inclui todos os recursos e etapas necessárias para as fases de planejamento, implementação e teste do processo de recuperação, e sobre todos os aspectos relevantes para a gestão da continuidade de negócios.

Usuários deste documento são os membros da alta direção e funcionários necessários para a recuperação desta atividade.

2. Reference documents

- Norma ISO/IEC 27001, cláusulas 7.4, A.5.29, A.5.30 e A.8.14
- Norma ISO 22301, cláusula 8.4.5
- [Lista de obrigações legais, regulamentares, contratuais e outras]
- [Procedimento de gestão de incidentes]
- [Procedimento de auditoria interna]

3. Premissas / limitações

Para que este Plano funcione, as seguintes condições devem ser atendidas:

- Todos os equipamentos, softwares e dados estão disponíveis como planejado na [documento]

Este Plano não cobre os seguintes tipos de incidentes:

- []

4. Informações gerais

Localização do site alternativo / Estratégia de recuperação	
---	--

Commented [AES4]: Este plano é escrito para organizações onde a recuperação da infraestrutura de TI e serviços de TI pode ser consolidada em um único plano.

Para organizações que possuem infraestrutura de TI complexa, ou possuem diferentes RTOs para diferentes sistemas de TI, pode ser melhor desenvolver Planos de recuperação de desastre separados para diferentes sistemas de TI.

Commented [AES5]: Se você não possui esta Lista, liste nestes marcadores toda a legislação e contratos que contenham requisitos para controle de acesso.

Commented [AES6]: Você pode encontrar um modelo para este documento na pasta "09_Controles_de_seguranca_do_Anexo_A_da_ISO_27001" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES7]: Você pode encontrar um modelo para este documento na pasta "12_Auditoria_interna" do Kit de documentação Premium da ISO 27001 e ISO 22301.

Commented [AES8]: Você também pode adicionar outras

Commented [AES9]: Especifique os documentos onde estes

Commented [AES10]: Você pode especificar aqui alguns

Commented [AES11]: Leia também este artigo:

Commented [AES13]: Copie da Estratégia de continuidade de negócios.

Commented [AES12]: As estratégias de recuperação poderiam ser, por exemplo:

- a) locais alternativos dentro da organização (por exemplo, se a própria organização tiver outros locais à sua disposição);
- b) locais alternativos que podem ser fornecidos por uma organização associada (por exemplo, se houver organizações associadas por propriedade que possuam locais alternativos adequados);

[nome da organização]

[nível de confidencialidade]

Objetivo de tempo de recuperação:	
Objetivo de ponto de recuperação:	
Personas responsáveis pela recuperação de dados de infraestrutura de TI (servidores, sistemas de arquivos, etc.):	
Personas que devem ser notificadas sobre o estado de dados, sistemas e infraestrutura:	
Personas responsáveis pela recuperação de dados de aplicativos de TI (clientes, fornecedores, parceiros, etc.):	
Atividades chave / obrigações / SLAs que devem ser atendidos e respectivos prazos:	
Capacidade mínima necessária para a recuperação de dados de TI:	
Personas que devem ser notificadas sobre o estado de dados, sistemas e infraestrutura:	

Commented [AES14]: Defina o tempo máximo dentro do qual a infraestrutura deve ser recuperada ou copie da Estratégia de continuidade de negócios.

Commented [AES15]: Defina o máximo de dados que podem ser perdidos, em termos de quantidade ou tempo.

Commented [AES16]: Pessoa especificada na parte principal

Commented [AES17]: Para saber mais sobre o assunto, leia este artigo:

Commented [AES18]: Geralmente todos os funcionários do

Commented [AES19]: Geralmente o chefe do departamento de TI.

Commented [AES20]: Geralmente o chefe do departamento de TI.

Commented [AES21]: O critério usual é que todas as

Commented [AES22]: Ex.: 80% dos usuários devem ter acesso

Commented [AES23]: Ex.: 20% dos usuários devem ter acesso total ao serviço logo após o desastre.

Commented [AES24]: Ex.: a operação normal deve ser retomada dentro de 12 horas após a ocorrência do desastre.

5. Papéis e informações de contato

Para o departamento de TI:

Num.	Papel na recuperação	Nome	Cargo / unidade organizacional	Telefone	Telefone Cel.	E-mail	Outros contatos	Outro e-mail
1.								
2.								
3.								
4.								
5.								

Commented [AES25]: Para saber mais sobre o assunto, leia este artigo:

Commented [AES26]: No caso de não haver telefone móvel

Commented [AES27]: Quem da lista atuará como substituto

Outras atividades na organização:

Commented [AES28]: Isto é departamentos comercial na organização.

[nome da organização]

[nível de confidencialidade]

Num.	Nome	Cargo / unidade organizacional	Telefone fixo	Telefone cel.	E-mail	Nível de confidencialidade
11.						
12.						
13.						
14.						
15.						

Contatos externos:

Num.	Nome da organização	Nome	Cargo / unidade organizacional	Telefone fixo	Telefone cel.	E-mail	Nível de confidencialidade
21.							
22.							
23.							
24.							
25.							

Commented [AES29]: Assegure de incluir o seguinte:

- Provedores de telecomunicação
- Fornecedores de hardware

6. Autorização em uma crise

Papel na recuperação / cargo	Autorização
Chefe do departamento de TI	Autorização para realizar todas as etapas especificadas no Plano de continuidade de negócios e neste Plano de recuperação de desastre de modo a recuperar a infraestrutura de TI / serviços de TI
[cargo]	Autorizado para compras urgentes de equipamento / serviços até [quantidade]
[cargo]	Autorizado a se comunicar com clientes
[cargo]	Autorizado a se comunicar com fornecedores de serviços terceirizados
[cargo]	Autorizado a negociar com fornecedores de tecnologia terceirizada de emergência
[]	

Commented [AES30]: Liste todas as outras autorizações

Nota: apenas o [cargo] está autorizado a se comunicar com o público através de mídias públicas

Commented [AES31]: Geralmente o CEO ou alguém da alta direção.

7. Evitando um Ponto único de falha

Os seguintes recursos substitutos serão usados para evitar um Ponto único de falha que possa causar uma interrupção:

Commented [AES32]: Exclua esta seção se o controle A.8.14

Ponto único de falha	Atividade onde ele ocorre	Nome do recurso afetado	Pessoa responsável por responder a essa falha

Commented [AES33]: Ex.: link de comunicação único, apenas

Commented [AES34]: Ex.: segundo link de comunicação, uma

Commented [AES35]: Esta coluna é usada para anotar a

8. Recursos necessários

Além dos recursos da seção anterior, os seguintes recursos serão usados para a recuperação desta atividade:

Nome do recurso	Descrição	Quantidade	Quando o recurso é necessário	Pessoa responsável pela obtenção do recurso
Pessoas:				
John Smith	Administrador de sistema	1	1 hora após a interrupção	Chefe da TI
Aplicações / bases de dados:				
Base de dados XYZ	Base de dados corporative	1	1 hora após a interrupção	Chefe da TI
Dados em formato eletrônico:				
Procedimento de RH da folha de pagamento	Descrição das etapas necessárias para realizar o processo de pagamento	1	5 horas após a interrupção	Analista de folha de pagamento

Commented [AES36]: Identifique quais recursos serão

Commented [AES37]: Descreva onde os recursos estão

Commented [AES38]: Esta coluna é usada para escrever

Commented [AES39]: Estes são apenas exemplos; exclua-os e

Commented [AES40]: Em particular, liste todos os dados de

Commented [AES41]: Estes são apenas exemplos; exclua-os e

Commented [AES42]: Estes são apenas exemplos; exclua-os e

Dados em papel:				
Registros de competência dos funcionários	Diplomas e certificados de cursos e treinamentos para o propósito de participação em licitações	1	1 semana após a interrupção	Chefe da TI
Equipamentos de TI e de comunicações:				
Servidor	Computador de alto desempenho	2	1 hora após a interrupção	Chefe da TI
Canais de comunicação:				
Outros equipamentos:				
Instalações e infraestrutura:				
Escritório de RH	Escritório alternativo para o pessoal de RH	1	3 horas após a interrupção	Chefe de instalações

Commented [AES43]: Estes são apenas exemplos; exclua-os e

Commented [AES44]: Estes são apenas exemplos; exclua-os e

Commented [AES45]: Estes são apenas exemplos; exclua-os e

Commented [AES46]: Estes são apenas exemplos; exclua-os e

[nome da organização]

[nível de confidencialidade]

Serviços externos:				

9. Etapas de recuperação para a infraestrutura de TI / serviços de TI

Esta atividade deveria ser recuperada da seguinte maneira:

Procedimentos de recuperação (etapas principais / tarefas individuais)	Pessoas responsáveis pela implementação		
[nome da etapa num. 1]			
...			
[nome da etapa num. 2]			
...			

10. Manutenção e revisão deste plano

A fim de manter a precisão e usabilidade deste Plano de recuperação de desastre, este plano será revisado e atualizado de acordo com a seguinte frequência:

Elemento de recuperação de desastre	Pessoa responsável pela revisão	Frequência
Disponibilidade de todos os recursos		

Commented [AES47]: Certifique-se de que você listou todos os

Commented [AES48]: Estes são apenas exemplos; exclua-os e

Commented [AES49]: Para saber mais sobre o assunto, leia este artigo:

Commented [AES50]: Comunicações geralmente são direcionadas a:

- Outras atividades / departamentos
- Equipe de gestão de crises
- Várias autoridades governamentais

Comunicação geralmente inclui:

- Notificação de que uma etapa foi implementada

Commented [AES51]: Esta coluna é preenchida apenas no

Commented [AES52]: Estas etapas devem levar em conta as diferentes estratégias que você definiu – por exemplo, etapas serão

Dependendo de sua infraestrutura de TI, você pode dividir seu plano em várias subseções que cobrirão, por exemplo:

- Plano de recuperação de PC's
- Comunicações de rede

Por exemplo, para o plano de recuperação de PC's, suas etapas poderiam ser as seguintes (você deveria adicionar tarefas mais detalhadas para cada uma destas etapas):

- 1) Os usuários devem notificar [seu coordenador] sobre as estações de trabalho que são requeridas
- 2) [seu coordenador] cria uma lista de todos os PC's e outros equipamentos juntamente com as configurações requeridas

Etapas de recuperação deveriam, entre outras etapas, incluir também o seguinte:

- Reunir a equipe no local alternativo e decidir como as pessoas indisponíveis serão substituídas
- Encontrar uma forma de prover suporte a todos os usuários de sistemas de informação

Commented [AES53]: Ex.: a cada 3 meses.

Commented [AES54]: Especifique aqui os elementos que você

[nome da organização]

[nível de confidencialidade]

...		
...		

Quando as atividades de revisão envolverem testes, os testes devem ser realizados de acordo com o [Procedimento de auditoria interna].

11. Gestão de registros mantidos de acordo com este documento

Nome do registro	Local de armazenamento	Responsável	Responsável de aprovação	Responsável de revisão
Registro da implementação da etapa de recuperação (registro em papel)	Arquivo [cargo]	[cargo]	[cargo]	[cargo]
Registro da revisão da etapa de recuperação (registro em formulário de papel)	Arquivo [cargo]	[cargo]	[cargo]	[cargo]

Commented [AES55]: Altere esses registros para combinar

Commented [AES56]: Geralmente o coordenador de

Commented [AES57]: Geralmente o coordenador de

Somente o [cargo] pode conceder a outros funcionários o acesso aos registros.

12. Validade e gestão de documentos

Este documento é válido a partir de [data].

Este documento, junto com todos os documentos adicionais, é armazenado da seguinte forma:

- os documentos em papel são armazenados nos seguintes locais: Centro de comando, [liste os locais]

Commented [AES58]: Geralmente é armazenado no local

Commented [AES59]: Armazene o documento para permitir o

O proprietário deste documento é o [cargo], que deve verificar e se necessário atualizar o documento como especificado na seção 10.

Ao avaliar a eficácia e adequação deste documento, os seguintes critérios precisam ser considerados:

- quantidade de ações corretivas baseadas nos exercícios conduzidos

- no caso de uma crise, se a recuperação foi completada dentro do objetivo de tempo de recuperação

13.Documentos adicionais

- [documentação técnica para sistemas de TIC]

• [documentação de processos]

[cargo]

[nome]

[assinatura]

Commented [AES60]: No caso de tal documentação ser

Commented [AES61]: Se as instruções de trabalho existentes

Commented [AES62]: Necessário somente se o Procedimento de controle de documentos e registros indicar que os documentos em papel devem ser assinados.