NORMA DE GESTÃO DE MUDANÇAS

1. OBJETIVO

Esta Norma tem o objetivo de assegurar a continuidade do negócio no ambiente produtivo, através da formalização dos procedimentos de mudanças, satisfazendo a orientação normativa do documento "Política de Segurança da Informação". Essa normatização fornece um mecanismo importante para acompanhamento e registro de todas as atividades relacionadas às mudanças que afetam sistemas e/ou infraestrutura.

2. ABRANGÊNCIA

Esta Norma aplica-se a toda e qualquer mudança referente a sistemas e/ou infraestrutura da ELUBEL.
Todos as pessoas de TI devem seguir essa norma.

3. ATRIBUIÇÕES E RESPONSABILIDADES

3.1. Departamento de Segurança da Informação e Infraestrutura

- 3.1.1. Realizar auditorias periódicas visando o cumprimento das diretrizes desta norma;
- 3.1.2. Tratar os incidentes de segurança abertos em função de não conformidades observadas;
- 3.1.3. Aplicar as Mudanças solicitadas conforme descrito nesta norma.
- 3.1.4. Garantir o armazenamento das documentações geradas nos processos de mudança

3.1. Departamento de Desenvolvimento

- 3.2.1. Observar e cumprir todas as diretrizes desta norma;
- 3.2.2. Garantir que as mudanças solicitadas sigam as melhores práticas informadas por essa norma;
- 3.2.3. Reportar quaisquer não conformidades através de abertura de incidente de segurança.

4. CONSIDERAÇÕES

Toda as mudanças devem considerar os seguintes pontos:

4.1. Propósito das Mudanças e suas potenciais consequências

- 4.1.1. Toda mudança deve ter um propósito claro e de necessidade imediata.
- 4.1.2. Toda mudança deve ser devidamente justificada e documentada.
- 4.1.3. Toda mudança deve descrever o problema que existe e que será corrigido ou informar se é a inclusão de um novo processo e/ou serviço.
- 4.1.4. Toda mudança deve descrever o procedimento para teste de validação e as ações que devem ser tomadas caso as alterações não surtam os efeitos esperados.

4.1.5. Toda mudança deve ter bem esclarecido as possíveis consequências da ação de mudança.

4.1.6. Mudanças referente a regras de firewall devem ser justificadas, informando IP de origem, destino, porta e protocolos.

4.1.7. Regras de firewall não podem ser feitas em âmbito genérico conforme descrito no documento **Norma de Gestão de Perímetro.**

5. INTEGRIDADE DE SISTEMAS

5.1.1. Mudanças relacionadas a sistemas e aplicações devem ser devidamente testadas e aprovadas antes de se gerar uma solicitação de mudança.

5.1.2. Toda mudança deve prezar pela integridade do sistema, informação, estrutura e continuidade de negócio.

5.1.3. As mudanças as serem realizadas devem ser pensadas, planejadas e sustentáveis a longo prazo.

5.1.4. Ao executar uma gestão de mudança deve se seguir a normativa do documento **Norma de Gestão de Vulnerabilidade.**

6. DISPONIBILIDADE DE RECURSOS

Toda mudança deve ser precedida de uma análise de quais recursos serão necessários para aplicar a mudança (pessoas, equipamentos, programas etc.) e quais recursos serão necessários para manter aquela alteração em operação (memória, HD, VPN etc.).

7. RESPONSABILIDADES

As mudanças devem ter pessoas designadas e responsáveis, apontando assim quem planejou, executou e aprovou a modificação. Deve-se ter claro também quem será o responsável por gerenciar, monitorar, controlar e/ou utilizar a nova aplicação.
A(s) pessoa(s) responsável(is) deve ficar atento para corrigir possíveis bugs e aplicar a melhoria continuada.

8. DIRETRIZES

Para uma melhor aplicação de controles, na ELUBEL as mudanças são classificadas como mudança programada e mudança emergencial.

8.1. Mudança Programada e Emergencial

8.2.1. **Mudança Programada** é o tipo de mudança que permite o planejamento antecipado e alinhamento entre todas as áreas envolvidas. A solicitação de mudança deve ser analisada e debatida entre as partes envolvidas pela mudança, para ser alinhada e aplicada dentro do período de mudanças programadas.

8.2.2. **Mudança emergencial** caracteriza-se por corrigir problemas graves que podem comprometer a continuidade operacional da ELUBEL. São exemplos de mudança emergencial: patches de aplicativos ou sistemas

operacionais que corrijam vulnerabilidades que já possuem exploração e que são categorizadas como Altas ou Críticas, patches dos sistemas desenvolvidos pela equipe da ELUBEL e corrijam falhas que podem permitir a concretização das ameaças, gerando incidentes etc.

A mudança programada e emergencial deve seguir o fluxo de aprovação descrito abaixo:

a) O solicitante da mudança deve formalizar o seu requerimento e encaminhar para aprovação do comitê de mudanças programadas.

b) A área de Segurança da Informação e Infraestrutura deve criar o plano de testes operacionais assim como o plano de retorno (rollback), e entregar esta documentação para o responsável pelos testes.

c) A área de Segurança da Informação e Infraestrutura deve validar o plano de testes e testar o plano de retorno (rollback).

d) Após a homologação da mudança em ambiente de testes, o responsável pela mudança neste ambiente deve emitir um termo de homologação e validação dos testes e encaminhar a mudança para a fase de produção.

e) O responsável pelo ambiente de produção deve aplicar a mudança em ambiente de produção e realizar as validações devidas.

f) Caso seja apresentada qualquer alteração no resultado deste teste, o plano de retorno (rollback) deve ser operacionalizado e as causas da falha devem ser investigadas. Uma vez identificadas as causas da falha e corrigido o problema, a mudança deverá ser testada e validada novamente no ambiente de produção.

g) O prazo para que a mudança classificada como programada seja colocada em produção, deve ser de no máximo seis meses ou no prazo estabelecido pelo solicitante, este prazo deve contemplar todos os passos supracitados.

h) Se a mudança foi classificada como emergencial para corrigir uma falha grave identificada nos sistemas que suportam as atividades críticas da ELUBEL, esta mudança deve ser realizada no período máximo de até 7 dias, não podendo ser feito o serviço deverá ser suspenso até a devida correção ou deverá ser assinado um termo de aceite de risco pela diretoria conforme documentos Planos de Resposta a Incidente e Política de Gestão de Risco.

9. RELATÓRIO

Toda última semana do mês, a equipe de Segurança da Informação e Infraestrutura, responsável por programar as mudanças no ambiente de produção, deve gerar um relatório de conformidade, relatando o status das implementações dos controles do referido mês.

10. SANÇÕES E PUNIÇÕES

O descumprimento dessa norma pode acarretar sanções e punições aos envolvidos.

11. REVISÕES

Está norma deverá ser revisada anualmente ou extraordinariamente, a qualquer momento se for necessário.