



NORMA DE GERENCIAMENTO DE SEGURANÇA

1. INTRODUÇÃO

Esta norma de segurança da informação serve para complementar a Política de Segurança da Informação, definindo as diretrizes para o uso aceitável e correto de ativos de informação da ELUBEL por seus usuários autorizados.

2. OBJETIVO

Estabelecer diretrizes para o uso aceitável e seguro ao que se refere aos ativos de informação da ELUBEL

3. ABRANGÊNCIA

Todos os empregados, sócios, colaboradores, terceiros que possuíram, possuem ou virão a possuir acesso às informações da ELUBEL ou fizeram, fazem ou farão uso de seus recursos computacionais.

4. ESCOPO

Esta norma segue o escopo definido previamente na Política de Segurança da Informação.

5. DIRETRIZES

- 5.1. Garantir que a Política de Segurança da Informação e os procedimentos adotados pela organização estejam compatíveis com a realidade.
- 5.2. Cobrar junto ao departamento de Segurança da Informação e Infraestrutura a implementação e documentação dos procedimentos definidos nas políticas de segurança e regulamentos.
- 5.3. Monitorar junto ao departamento de Segurança da Informação e Infraestrutura e analisar os alertas de segurança da informação para garantir a confidencialidade, integridade e disponibilidade das informações.
- 5.4. Implementar um programa formal de conscientização da segurança de modo a disseminar a importância atribuída à segurança dos dados.
- 5.5. Cobrar a manutenção de procedimentos periódicos de segurança operacionais, administrativos e técnicos que sejam compatíveis com a LGPD.
- 5.6. Realizar o processo de avaliação de risco, identificando ameaças e vulnerabilidades, gerando relatórios com os resultados conclusivos sobre as avaliações de risco.
- 5.7. Criar e distribuir planos de resposta de incidente de segurança e procedimentos de escalonamento.
- 5.8. Definir estratégia de comunicação e definição de responsabilidades.
- 5.9. Informar sobre incidentes de dados pessoais e fazer um anúncio público relatando o ocorrido e as medidas tomadas.
- 5.10. A área de segurança da informação deve gerenciar as contas de usuários, incluindo adições, exclusões e modificações



- 5.11. A área de segurança da informação deve manter procedimentos de resposta a incidentes, escalonamento atualizados, assegurando a administração oportuna e eficiente de todas as situações
- 5.12. A área de segurança da informação deve controlar o acesso aos dados relevantes.
- 5.13. A área de segurança da informação, deve executar periodicamente os planos de resposta a incidente de segurança e processo de escalonamento.
- 5.14. A área de segurança da informação, deve monitorar todos os pontos de saída da rede e implantar um DLP (Data Loss Prevention).
- 5.15. Definir e manter responsabilidades de resposta aos alertas e incidentes de segurança.
- 5.16. Treinar os participantes dos planos de resposta a incidentes, quanto as suas responsabilidades pela resposta a uma quebra de segurança.
- 5.17. Prevenir intrusão e alertar caso seja detectada alguma anomalia na integridade dos dados.
- 5.18. Cobrar as áreas para que faça o descarte dos dados periodicamente e imediatamente quando solicitado pelo cliente, conforme apontado na norma de armazenamento e descarte de dados.
- 5.19. Garantir que os prestadores de serviços cumpram com as exigências desta norma e as regras da LGPD.
- 5.20. Formalizar acordo que inclua uma confirmação de que os prestadores de serviço são responsáveis pela segurança dos dados pessoais.
- 5.21. Formalizar um acordo de confidencialidade de todas as informações na empresa, principalmente dos dados pessoais e dados pessoais sensíveis, com todos os colaboradores e prestadores de serviço.
- 5.22. A responsabilidade pela segurança da informação na ELUBEL é de todos os envolvidos com as operações da ELUBEL, no qual todos tem um papel fundamental para garantir a confidencialidade, integridade e disponibilidade das informações.

6. RESPOSTAS A INCIDENTES

- 6.1. As pessoas designadas estarão de plantão para responder a incidentes na plataforma, seja de segurança ou operacional.
- 6.2. A relação de pessoas aptas a estarem de plantão descrito no Anexo I, deverá ser atualizada sempre que houver mudanças no quadro de colaboradores ou nas atividades que cada colaborador desempenha.

7. SANÇÕES E PUNIÇÕES

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

8. REVISÕES

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



9. ANEXOS

Anexo I

Usuário	Cargo	Nível de Acesso	Telefone
		Acesso total ao ambiente.	
		Acesso total ao ambiente.	
		Acesso total ao ambiente.	
		Acesso total ao ambiente	