POLÍTICA DE ARMAZENAMENTO, ANONIMIZAÇÃO E DESCARTE

1. INTRODUÇÃO

Essa Norma de Segurança da Informação serve para complementar a Política de Segurança da Informação, definindo as diretrizes para o devido armazenamento, manuseio e descarte de informações da ELUBEL.

2. OBJETIVO

Estabelecer diretrizes para o devido armazenamento, manuseio e descarte de informação da ELUBEL

3. ABRANGÊNCIA

Todos os empregados, sócios, colaboradores, terceiros que tenham acesso a informações da ELUBEL devem seguir essa norma.

4. ESCOPO

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

5. DIRETRIZES

5.1. A informação é um ativo muito importante para a ELUBEL, por isso, todos os colaboradores e prestadores de serviços devem adotar comportamento seguro ao armazenar, manusear e descartar qualquer tipo de informação.

5.2. Diretores, gerentes, coordenadores, colaboradores, parceiros e prestadores de serviços devem assumir atitude proativa no que diz respeito a proteção das informações da ELUBEL.

5.3. Todo o acesso à informação da ELUBEL que não for explicitamente autorizado é proibido.

5.4. Informações confidenciais da ELUBEL não devem ser transportadas em qualquer tipo de mídia sem as devidas proteções e autorizações.

5.5. As informações devem ser classificadas conforme a tabela abaixo:

Níveis de Classificação	Características
Pública	Informações que podem ou devem ser divulgadas publicamente. A divulgação deste tipo de informação não causa problemas a ELUBEL ou ao titular dos dados e parceiros, podendo ser compartilhada livremente com o público em geral, desde que seja mantida sua integridade. Fica a critério da ELUBEL designar alguém ou um setor para divulgações públicas. A classificação dessa informação continua sendo uma responsabilidade do gestor.

Interna	Informações internas são aquelas divulgadas a todos os colaboradores e prestadores de serviços, desde que estes estejam comprometidos com a confidencialidade das informações.
Reservada	Informações confidencial são aquelas restritas a um determinado grupo, área ou cargo, que necessitem conhecê-las para o desempenho de suas tarefas profissionais na ELUBEL Exemplos são projetos, relatórios, indicadores e outros
Secreta/Confidencial	Informações Secretas/Confidenciais são aquelas que requerem um tratamento especial, pois cuja divulgação não autorizada ou acesso indevido, pode gerar prejuízos financeiros, legais, normativos, contratuais ou na reputação, imagem ou estratégia da ELUBEL Exemplos são informações privadas de pessoas, fornecedores e informações estratégicas.

5.6. Documentos importantes ou confidenciais devem ser devidamente guardado e protegido, tendo acesso restrito.

5.7. A transferência de dados pessoais para dispositivos removíveis é proibida.

5.8. Dúvida sobre a Política e Normas de Segurança da Informação devem ser imediatamente esclarecidas com o gestor responsável, ou com a área de segurança da informação.

5.9. Em períodos de ausência da estação de trabalho, documentos em suporte físico devem ser retirados das mesas e de outras áreas de superfície.

5.10. Documentos de uso interno ou confidenciais em suporte eletrônico devem ser armazenados em ambientes com acesso controlado e senhas para impedir o acesso de pessoas não autorizadas.

5.11. Todo o armazenamento, manuseio e descarte de informações da empresa, cliente ou colaboradores, deverá ser feita de forma segura para evitar vazamento de dados que poderá trazer ônus a empresa. Para isso seguir as seguintes instruções:

5.11.1. Armazenamento

5.11.1.1. Todas as informações de suporte físico, categorizada como confidencial deve ser guardado em gavetas ou armários trancados de forma a impedir o acesso de pessoas não autorizadas.

5.11.1.2. Todas as informações internas e confidenciais de suporte eletrônico deve ser armazenado em ambiente com acesso controlado e com senha impedindo o acesso de pessoas não autorizadas, além de registro de acesso.

5.11.1.3. Todos os dados pessoais salvos na nossa base de dados, devem ser fornecidos voluntariamente e conscientemente pelo usuário e deixando claro a sua utilização.

5.11.1.4. Os dados e/ou documentos com suporte físico, deverão ser armazenado em um local seguro com acesso restrito apenas para pessoas autorizadas. Conforme o item 5.11.1.

5.11.1.5. Documentos, informações, dados pessoais, pertencentes a ELUBEL que forem armazenados em mídias móveis como Pen drive, HD, BD, DVD, CD dentre outros, deverá ter obrigatoriamente uma criptografia de alto nível e senha de alto nível.

5.11.1.6. Servidor ou banco de dados que armazenar informações, dados e documentos, tem que estar com a trilha de auditoria ativada para geração de log de acesso.

5.11.1.7. Todos os dados de autenticação, devem ser armazenados para fazer recorrência, única exceção à regra é o não armazenado do CVV.

5.11.1.8. Somente devem ser armazenados os dados estritamente necessários, todo o resto deve ser descartado após a utilização

5.11.2. Anonimização

5.11.2.1. A anonimização de dados é a prática de tratamento de dados que visa impossibilitar a identificação das pessoas relacionadas às informações. Os dados adequadamente anonimizados podem ser utilizados livremente, estando excluídos do escopo de aplicação de qualquer penalidade legal.

5.11.2.2. Neste sentido, quando a identificação do titular do dado não for essencial ou necessária para um determinado processo, tal como uma pesquisa interna ou externa, deverá ser feita a sua anonimização, a fim de que seja impossível o seu reconhecimento, mantendo-se as informações que são necessárias para fins estatísticos, desde que não haja qualquer tipo de possibilidade de se reconhecer o titular do dado.

5.11.2.3. Poderá ser utilizado qualquer método de anonimização, desde que torne a recuperação de dados pessoais impossível.

5.11.3. Descarte

5.11.3.1. Os dados digitais e/ou documentos impressos, categorizados como confidenciais, deverão ser triturados e/ou incinerados, caso seja um grande volume de documentos deverá ser realizado através de uma empresa ilibada de descarte de dados, que emita um certificado de eliminação de documentos seguro. Para exemplificar, acesse o Anexo I.

5.11.3.2. Cada departamento depois de categorizar os documentos deverá estipular um período para o descarte da informação, fazendo assim um descarte de dados periodicamente. Esse plano periódico de descarte deve ser documentado e informado a equipe de segurança para fazer o devido monitoramento.

5.11.3.3. Dispositivos que possuam informações classificadas como nível de confidencialidade elevado, deve ser destruído fisicamente ou as informações devem ser destruídas, utilizando técnicas que torne a recuperação de dados impossível. Para exemplificar olhar Anexo I.

5.11.3.4. Documentos de baixa relevância pode utilizar processo de descarte mais simples. Para exemplificar olhar o Anexo I.

5.11.3.5. Documentos, informações e dados pessoais pertencentes a ELUBEL, que armazenado em mídia móvel como Pen drive, HD, BD, CD, DVD dentre outros, quando forem descartados, deverá ser destruído logicamente se não forem dados públicos, caso sejam dados categorizados como confidencial, deverá preferencialmente fazer o descarte físico através de pulverização, desintegração, trituração e/ou incineração. Para exemplificar olhar Anexo I.

5.11.3.6. Os dados pessoais deverão ser excluídos em um prazo de até 7 dias corridos, quando solicitado pelo titular do dado, desde que de acordo com as premissas de segurança e regulatórias.

5.11.3.7. Os itens de descarte deverão ser registrados sempre que possível para uma auditoria se necessário, seguindo os seguintes parâmetros:

5.11.3.7.1. **Descarte via solicitação do Titular do Dado:** Deverá ser gerado um número de protocolo ou similar que será fornecido ao titular. Nos registros deverá conter o protocolo, data, quantidade de dados descartados e número do solicitante.

5.11.3.7.2. **Troca ou Descarte do Desktop:** Deverá ser registrado o modelo e marca do equipamento, usuário antigo e destino do equipamento. Além de registrar a data que foi executado o procedimento cabível de descarte de dados.

5.11.3.7.3. **Destruição dos dados via terceiro:** Informar o tipo de equipamento ou documento, quantidade se aplicável, método de destruição e comprovante da destruição.

6. SANÇÕES E PUNIÇÕES

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

7. REVISÕES

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

Anexo I

Método	Descrição	Aplicável a	Categoria do Dado
Excluir	Excluir dados de mídias de armazenamento magnético ou na rede. Esse método não destrói fisicamente a mídia.	Discos rígidos, disquetes, fitas, flash disk, discos removíveis, CD, DVD, BD e similares	Pública
Sob escrever mídia	Sob escrever dados em mídias de armazenamento magnético, por pelo menos 07 vezes utilizando método Dod 5220.22M para dados internos e Gutmann para dados confidenciais. Este método não destrói fisicamente a mídia.	Discos rígidos, disquetes, fitas, flash disk, discos removíveis, CD, DVD, BD e similares	Interno e Confidencial
Destruição Física	Destruição física da mídia de armazenamento através da pulverização, desintegração, trituração e/ou incineração. Este método destrói completamente a mídia e todos os dados.	Discos rígidos, disquetes, fitas, flash disk, discos removíveis, CD, DVD, BD e similares	Confidencial
Desmagnetização	Desmagnetização de mídias como fitas, HDs e disquetes Este método destrói todos os dados e inviabiliza a reutilização do equipamento.	Disco rígido, disquetes, fitas, flash disks e disco removíveis.	Confidencial