# SEGURANÇA DA INFORMAÇÃO

Para reduzir o risco de ocorrências de falhas prejudicarem de algum modo a Adega UniBeer, as informações devem ser adequadamente utilizadas, armazenadas e protegidas. Sendo assim, as propriedades que devem ser preservadas para garantir a segurança das informações são as seguintes:

• Confidencialidade: garante que a informação estará disponível somente para as pessoas, entidades ou processos autorizados;

• Integridade: garante que a informação não pode ser alterada ou destruída sem a autorização adequada;

• Disponibilidade: possibilita que os recursos estejam sempre acessíveis, ao ser solicitado por uma entidade autorizada.

**Adega UniBeer – LGPD**

A **Lei Geral de Proteção de Dados Pessoais (LGPD), Lei n° 13.709/2018**, foi promulgada para proteger os direitos fundamentais de liberdade e de privacidade e a livre formação da personalidade de cada indivíduo. A Lei fala sobre o tratamento de dados pessoais, dispostos em meio físico ou digital, feito por pessoa física ou jurídica de direito público ou privado, englobando um amplo conjunto de operações que podem ocorrer em meios manuais ou digitais.

No âmbito da LGPD, o tratamento dos dados pessoais pode ser realizado por dois agentes de tratamento, o **Controlador** e o **Operador**. Além deles, há a figura do **Encarregado**, que é a pessoa indicada pelo Controlador para atuar como canal de comunicação entre o Controlador, o Operador, os(as) titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).

Tema fundamental trabalhado pela Lei, o **tratamento de dados** diz respeito a qualquer atividade que utiliza um dado pessoal na execução da sua operação, como, por exemplo: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

Antes de iniciar qualquer tipo de tratamento de dados pessoais, o agente deve se certificar que a finalidade da operação está registrada de forma clara e explícita e os propósitos especificados e informados ao(à) titular dos dados. No caso do setor público, a principal finalidade do tratamento está relacionada à execução de políticas públicas, devidamente previstas em lei, regulamentos ou respaldadas em contratos, convênios ou instrumentos semelhantes.

O compartilhamento dentro da administração pública, no âmbito da execução de políticas públicas, é previsto na Lei e dispensa o consentimento específico. Contudo, o órgão que coleta deve informar com transparência qual dado será compartilhado e com quem. Do outro lado, o órgão que solicita receber o compartilhamento precisa justificar esse acesso com base na execução de uma política pública específica e claramente determinada, descrevendo o motivo da solicitação de acesso e o uso que será feito com os dados. Informações protegidas por sigilo seguem protegidas e sujeitas a normativos e regras específicas. Essas e outras questões fundamentais devem ser observadas pelos órgãos e entidades da administração federal no sentido de assegurar a conformidade do tratamento de dados pessoais de acordo com as hipóteses legais e princípios da LGPD.

A Lei estabelece uma estrutura legal de direitos dos(as) titulares de dados pessoais. Esses direitos devem ser garantidos durante toda a existência do tratamento dos dados pessoais realizado pelo órgão ou entidade. Para o exercício dos direitos dos(as) titulares, a LGPD prevê um conjunto de ferramentas que aprofundam obrigações de transparência ativa e passiva, e criam meios processuais para mobilizar a Administração Pública.

Documento base:  [**Guia de Boas Práticas para Implementação na Administração Pública Federal da Lei Geral de Proteção de Dados**](https://www.gov.br/governodigital/pt-br/seguranca-e-protecao-de-dados/guias/guia_lgpd.pdf), documento elaborado pelos diferentes órgãos que compõem o Comitê Central de Governança de Dados e que contém orientações sobre as atribuições e atuação do Controlador, do Operador e do Encarregado, bem como da Autoridade Nacional de Proteção de Dados (ANPD) e versa, ainda, sobre os direitos fundamentais dos(as) cidadãos(ãs) titulares dos dados, aborda hipóteses de tratamento dos dados e sua realização, indica o ciclo de vida do tratamento dos dados pessoais e apresenta boas práticas em segurança da informação.

**Sistema de backups**

* garantir que o backup programado está sendo realizado na frequência adequada (completo, diferencial ou incremental);
* garantir a integridade dos dados nas cópias de segurança;
* garantir o correto armazenamento das cópias, seja em mídias físicas ou na nuvem;
* realização de testes contínuos de verificação dos dados que são copiados e armazenados, identificando e corrigindo erros;
* geração de relatórios diários e da correta documentação dos mesmos, incluindo problemas e dados salvos;
* a depender das informações em questão, promover o atendimento e o alinhamento a normas regulatórias, a exemplo da LGPD – Lei Geral de Proteção de Dados.

**Política de uso de E-mail**

O correio eletrônico é fundamental para funcionamento da empresa, pois permite a comunicações entre os vários departamentos da empresa e colaboradores internos facilitando o processo, também é monitorado pela equipe de T.I.

O uso do e-mail corporativo é responsabilidade do colaborador. As mensagens enviadas não podem conter:

* Conter linguagem ofensiva
* Trazer prejuízos a outras pessoas
* Conter conteúdos obscenos
* Vazar informações sigilosas da empresa

**Descarte de informações e mídia**

Para impedir que as informações sigilosas da empresa armazenadas nos equipamentos ou mídias sejam acessadas por agentes não autorizados, é importante que uma conduta do descarte correto de unidade de mídia e equipamentos seja seguida.

A eliminação segura acontece por meio da destruição ou deletar as informações que estão contidas nos equipamentos ou mídias, com o objetivo tornar as informações irrecuperáveis.

**Admissão e Demissão de colaboradores**

O Setor de departamento financeiro e pessoal deverá sempre informar ao setor de TI, a entrada e saída de colaboradores na empresa, o setor de TI ficará responsável pela criação de usuários e exclusão.

No caso de demissão, o colaborador deverá entregar todos os pertencentes da empresa, que ficou sobre sua responsabilidade durante o período trabalhado e ainda terá seus acessos excluídos do sistema, se ainda continuar tendo acessos as informações da empresa serão encaminhadas notificações ao departamento pessoal e financeiro solicitar a exclusão.

**Cópias de seguranças**

É imprescindível fazer a realização de backups diariamente na empresa para prevenir ataques de ransomwares e outros ataques cibernéticos, também proteger dados essenciais da empresa, por isso o setor de T.I criou um espaço de armazenamento que é protegido com senha, só é acessado quem possui a senha, a senha deve ter no mínimo 6 caracteres que é criada pelo usuário, esse espaço permite que os colaboradores possam fazer uploads de informações pessoais e corporativas que serão convertidos automaticamente em criptografia em servidores específicos da empresa.

**Controle contra Malware**

Todos os computadores corporativos da empresa vão ter antivírus instalado no processo de configuração. Setor de T.I fará a administração e o controle do antivírus, fazendo atualizações, manutenção e preventivas, o antivírus irá automaticamente fazer uma varredura diariamente garantindo que estejam livres e seguras de possíveis intrusos no sistema.