Política de

Segurança da Informação

VINÍCOLA
AURORA

SUMÁRIO

1. Introdução

A Cooperativa Vinícola Aurora compreende que a manipulação de sua informação passa por diferentes meios de suporte, armazenamento e comunicação, sendo estes vulneráveis a fatores externos e internos que podem comprometer a segurança das informações corporativas.

Dessa forma, a Cooperativa Vinícola Aurora estabelece sua Política de Segurança da Informação, como parte integrante do seu sistema de gestão corporativo, alinhada as boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção às informações da organização ou sob sua responsabilidade.

2. Propósito

Esta política tem como propósito:

2.1. Estabelecer diretrizes e normas de Segurança da Informação que permitam aos colaboradores da Cooperativa Vinícola Aurora adotar padrões de comportamento seguros, adequados às metas e necessidades da Cooperativa Vinícola Aurora;

2.2. Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

2.3. Resguardar as informações da Cooperativa Vinícola Aurora, garantindo requisitos básicos de confidencialidade, integridade e disponibilidade;

2.4. Prevenir possíveis causas de incidentes e responsabilidade legal da instituição e seus colaboradores, clientes e parceiros;

2.5. Minimizar os riscos de perdas financeiras, de participação no mercado, da confiança de clientes ou de qualquer outro impacto negativo no negócio da Cooperativa Vinícola Aurora como resultado de falhas de segurança.

3. Escopo

Esta política se aplica a todos os usuários da informação da Cooperativa Vinícola Aurora, incluindo qualquer indivíduo ou organização que possui ou possuiu vínculo com a Cooperativa Vinícola Aurora, tais como colaboradores, ex-colaboradores, prestadores de serviço, ex-prestadores de serviço, que possuíram, possuem ou virão a possuir acesso às informações da Cooperativa Vinícola Aurora e/ou fizeram, fazem ou farão uso de recursos computacionais compreendidos na infraestrutura Vinícola Aurora.

Durante as atividades de tratamento de dados pessoais, as diretrizes da presente Política devem ser observadas em conjunto com as diretrizes constantes na Política Geral de Proteção de Dados Pessoais, eis que absolutamente complementares.

Esta política é aplicável no âmbito do grupo da Cooperativa Vinícola Aurora, qual seja:

Cooperativa Vinícola Aurora Ltda - Matriz Rua Olavo Bilac, 500 - Cidade Alta 95700-362 - Bento Gonçalves - RS CNPJ: 87.547.188/0001-70	Cooperativa Vinícola Aurora Ltda - Filial Porto Alegre Rua Dr. Timóteo, 374 - Conjuntos 406 e 407 - Bairro Floresta 90570-040 - Porto Alegre - RS CNPJ: 87.547.188/0017-38
Cooperativa Vinícola Aurora Ltda - Unidade 2 Rua Assis Brasil, 613 - Centro 95703-050 - Bento Gonçalves - RS CNPJ: 87.547.188/0059-97	Cooperativa Vinícola Aurora Ltda - Filial São Paulo Av. Brig. Luiz Antônio, 4556 - Bairro Jardim Paulista 01402-002 - São Paulo - SP CNPJ: 87.547.188/0019-08
Cooperativa Vinícola Aurora Ltda - Unidade Vinhedos RODOVIA RS 444, 1575- Linha Rui Barbosa 95701-430 - Bento Gonçalves - RS CNPJ: 87.547.188/0009-28	Cooperativa Vinícola Aurora Ltda - Filial Rio de Janeiro Rua Paulo e Silva, 30 - Bairro São Cristóvão 20910-120 - Rio de Janeiro - RJ CNPJ: 87.547.188/0020-33
Cooperativa Vinícola Aurora Ltda - Filial Brasília SBN Q 02 LT 12 BL F SL 705 70040-911 - Brasília - DF CNPJ: 87.547.188/0006-85	

4. Legislação de referência

4.1. ABNT NBR ISO/IEC 27001/ 2013 e ISO/IEC 27701/2019

4.2. LGPD 13.709/2018

4.3. Marco Civil da Internet 12.965/2014

5. Conceitos

Segurança da Informação	**A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações.**
Confidencialidade:	Toda informação deve ser protegida de acordo com o grau de sigilo de seu conteúdo, visando a limitação de seu acesso e uso apenas às pessoas autorizadas
Integridade:	Toda informação deve ser mantida na mesma condição em que foi disponibilizada pelo seu proprietário, visando protegê-la contra alterações indevidas, intencionais ou acidentais.
Disponibilidade:	Toda informação deve estar disponível aos seus usuários de forma oportuna e confiável.

Incidente de Segurança da Informação:	Um evento ou uma série de eventos indesejados ou inesperados que podem gerar impacto sobre a confidencialidade, integridade ou disponibilidade das informações e que podem comprometer as operações do negócio.
Violação de Dados Pessoais:	Todo incidente de Segurança da Informação que resulta na violação da integridade, disponibilidade ou confidencialidade de dados pessoais.
Ativo:	Qualquer bem, material ou intangível, dotado de valor para a organização.
BYOD (*Bring Your Own Device*):	Traduzido literalmente como “traga seu próprio dispositivo móvel”, refere-se à utilização de dispositivos pessoais no ambiente de trabalho.
Backup	Cópias de segurança de arquivos para um armazenamento Secundário, buscando a preservação dos dados em caso de problemas com a cópia principal.
Gestor da Informação:	Os gestores da informação são os membros da diretoria e gerência da Cooperativa Vinícola Aurora Ltda.
Gestor do Usuário	Os gestores do Usuário são os membros da diretoria e gerência da Cooperativa Vinícola Aurora Ltda que possuem colaboradores sob a sua gestão.
Informação Confidencial	Informações confidenciais somente devem ser acessadas por aqueles com reais necessidades de seu conhecimento para desempenhar suas atividades junto à organização. O acesso a esta informação deve ser monitorado. O acesso indevido a esta informação pode causar sérios problemas à organização, tais como perdas financeiras, prejuízo à imagem perante os clientes, vantagem estratégica de concorrentes, entre outros. Exemplo: planejamentos estratégicos, contratos com parceiros de negócio, dados pessoais e dados pessoais sensíveis, etc.
Informação Interna	Esta informação é compreendida como de acesso e uso da Cooperativa Vinícola Aurora

	Ltda e, em alguns casos, de seus parceiros de negócio, sendo proibido seu acesso público. O acesso de outros a estas informações pode prejudicar a Cooperativa Vinícola Aurora Ltda, seus colaboradores e seus parceiros de negócio. Informações classificadas como de Uso Interno podem ser relatórios, planilhas de controle, lista de telefones, entre outros.
Informação Pública	O acesso público a esta informação não causa qualquer problema para a Cooperativa Vinícola Aurora Ltda, seus colaboradores ou seus parceiros de negócio. Qualquer informação somente poderá ser divulgada ao público se possuir esta categoria de classificação, definida pelo gestor da informação. Exemplo: material de marketing e material postado na página da Cooperativa Vinícola Aurora Ltda na Internet.

6. Diretrizes

O objetivo da gestão de Segurança da Informação da Cooperativa Vinícola Aurora é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte as operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos a instituição.

A Presidência, Diretoria e o Comitê Gestor da Segurança da Informação estão comprometidos com uma gestão efetiva de Segurança da Informação na Cooperativa Vinícola Aurora. Desta forma, adotam todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida em todos os níveis da organização. Comprometem-se e responsabilizam-se com a melhoria contínua da gestão da Segurança da Informação.

A alta direção da Cooperativa Vinícola Aurora também apoia e se compromete com a conformidade com a legislação e as regulamentações de proteção de dados e com os termos contratuais acordados com os parceiros.

7. Classificação e tratamento da informação

7.1. Manipulação de Informações

Todos os usuários devem observar os requerimentos de manipulação das informações, baseando-se em sua classificação de segurança e sensibilidade, conforme descrito nesta política.

Todo o usuário ou colaborador é responsável por garantir a segurança da informação confidencial sob sua guarda, com o objetivo de evitar que a mesma possa ser lida, copiada ou extraviada por pessoa não autorizada.

Dados Pessoais e **dados pessoais sensíveis** devem ser classificados e tratados como **informações confidenciais.**

7.2. Reprodução das Informações

Informações copiadas devem manter a classificação dos originais e consequentemente os mesmos requisitos definidos para sua classificação. Os seguintes aspectos devem ser seguidos no que diz respeito à cópia de informações:

a) **informações confidenciais:** informações confidenciais somente devem ser copiadas sob autorização do Gestor da Informação e o acesso à cópia somente deve ser liberado para funcionários da organização;

b) **informações internas:** informações internas podem ser copiadas livremente porém o acesso à cópia somente deve ser liberado para funcionários da organização;

c) **informações públicas**: informações públicas são consideradas livres para cópia por qualquer pessoa.

7.3. Armazenamento das Informações

a) **Informações confidenciais:**

em papel: informações confidenciais em papel devem ser armazenadas em locais protegidos contra acesso físico. Devem ser armazenadas em armários com chaves ou locais que permitam que apenas pessoas autorizadas acessem a informação;

em mídia digital: informações confidenciais digitais devem ser armazenadas na rede corporativa. Estas informações somente podem ser transmitidas após autorização do Gestor da Informação. Controles adicionais podem ser requeridos pelo mesmo para proteger a informação, tais como proteção por senha de acesso, criptografia, entre outros. Quando armazenadas em mídias removíveis (CDs, Pen Drives, fitas, etc.), estas informações devem estar protegidas contra acesso de terceiros. Armários com chaves ou locais que permitam o acesso apenas de pessoas autorizadas devem ser utilizados;

b) **Informações internas**:

em papel: informações internas em papel devem ser armazenadas em locais protegidos do acesso de terceiros;

em mídia digital: informações internas digitais devem ser armazenadas na rede corporativa. Quando armazenadas em mídias removíveis, estas devem estar protegidas contra acesso de terceiros;

c) **Informações públicas:**

em papel: informações públicas não possuem restrições quanto ao armazenamento;

em mídia digital: informações públicas não possuem restrições quanto ao armazenamento;

em som: informações públicas não possuem restrições quanto ao armazenamento;

em imagem: informações públicas não possuem restrições quanto ao armazenamento.

7.4. Transmissão pelo Correio Convencional

a) **Informações confidenciais:**

em papel: informações confidenciais em papel devem ser transmitidas somente após aprovação do Gestor da Informação. Controles de segurança adicionais podem ser requeridos pelo mesmo, tais como utilização de envelope lacrado descrevendo emissor e destinatário, utilizando apenas serviços que garantam a entrega em mãos ao destinatário definido pelo emissor da informação;

em mídia digital: informações confidenciais em mídia digital devem ser transmitidas somente após aprovação do Gestor do Usuário. Controles de segurança adicionais podem ser requeridos pelo mesmo, tais como utilização de embalagem lacrada descrevendo emissor e destinatário, utilizando apenas serviços que garantam a entrega em mãos ao destinatário definido pelo emissor da informação;

b) **Informações internas:**

em papel: informações internas em papel somente podem ser enviadas para fora da organização após aprovação do Gestor da Informação. Internamente a transmissão destas informações é livre;

em mídia digital: informações internas em mídia digital somente podem ser enviadas para fora da organização após aprovação do Gestor da Informação. Internamente a transmissão destas informações é livre;

c) **Informações públicas:**

em papel: não existem restrições para a transmissão de informações públicas pelo correio;

em mídia digital: não existem restrições para a transmissão de informações públicas pelo correio;

em som: não existem restrições para a transmissão de informações públicas pelo correio;

em imagem: não existem restrições para a transmissão de informações públicas pelo correio.

7.5. Transmissão pelo Correio Eletrônico

a) **Informações confidenciais:**
formatos aplicáveis: informações confidenciais devem ser transmitidas via correio eletrônico somente após aprovação do Gestor da Informação. Arquivos de computador devem possuir senha de proteção sempre que possível.

b) **Informações internas:**
formatos aplicáveis: Informações internas somente podem ser transmitidas através de correio eletrônico para fora da organização após aprovação do Gestor da Informação. Internamente a transmissão destas informações é livre;
imagem: informações internas em imagem somente podem ser enviadas para fora da organização após aprovação do Gestor da Informação. Internamente a transmissão destas informações é livre.

c) **Informações públicas:**
formatos aplicáveis: não existem restrições para a transmissão de informações públicas pelo correio eletrônico.

7.6. Transmissão pela Fala

a) **Informações confidenciais:**
em conversas: Tais informações somente podem ser transmitidas em conversas a pessoas envolvidas com o processo em questão e autorizadas pelo Gestor da Informação;
em aparelhos telefônicos: seguem a mesma regra da transmissão em conversas.

b) **Informações internas:**
em conversas: Tais informações podem ser transmitidas em conversas a pessoas internas ao ambiente organizacional;
em aparelhos telefônicos: informações internas somente devem ser transmitidas através de conversas telefônicas entre aparelhos pertencentes à organização.

c) **Informações públicas:**
em formatos aplicáveis: não existem restrições para a transmissão de informações públicas através da fala.

7.7. Destruição da Informação

A definição do prazo de guarda/retenção e a destruição de documentos, obrigatoriamente, deverá seguir as determinações da Norma de Retenção e Descarte e o prazo registrado na Tabela de Temporalidade.

a) **Informações confidenciais:**
em papel: informações confidenciais em papel devem ser destruídas de maneira a impossibilitar a recuperação de informações. Informações confidenciais impressas na organização devem ser descartadas através de picotadores de papel ou incinerados pela organização;

em mídia digital: mídias digitais que contêm informações confidenciais devem ser destruídas de forma a impossibilitar a recuperação das informações. Informações sobre o descarte de mídias digitais podem ser obtidas junto ao Setor de Tecnologia da Informação;

b) **Informações internas**
em papel: devem ser destruídas de maneira a impossibilitar a recuperação de informações;

em mídia digital: mídias digitais que contêm informações internas devem ser destruídas de forma a impossibilitar a recuperação das informações. Informações sobre o descarte de mídias digitais podem ser obtidas junto ao Setor de Tecnologia da Informação. Informações sobre o descarte destes tipos de informações podem ser obtidas junto ao Setor de Tecnologia da Informação.

c) **Informações públicas**
em papel: não existem restrições para a destruição de informações públicas;
em mídia digital: não existem restrições para a destruição de informações públicas;

8. Controles

8.1. Acesso Físico

Todos que possuem acesso às estruturas da Cooperativa Vinícola Aurora Ltda, não importando sua condição (consultor, temporário e terceiro), devem ser atendidos e ter o acesso autorizado pela recepção da Cooperativa Vinícola Aurora Ltda.

Alterações nas garantias de acesso de funcionários ou colaboradores somente podem ser requeridas pela gerência responsável, alterando-se o formulário de "Termo de Compromisso e Responsabilidade sobre o uso de Recursos de Informática e outros".

8.2. Acesso Lógico

Baseado em um mapeamento de cargo/função, o Gestor do Usuário solicita o acesso lógico do mesmo ao Setor de Tecnologia da Informação através do Termo de Compromisso e Responsabilidade sobre o uso de Recursos de Informática e outros. Se houver alguma exceção no acesso deste determinado usuário, seu Gestor deve encaminhar ao Gestor da Informação para que esta particularidade seja autorizada.

São identificados quem tem acesso aos arquivos Confidenciais, Internos e Públicos. Também os perfis de acesso aos sistemas e o que contempla a nível de sistemas cada um desses perfis. Nenhum acesso pode ser concedido a qualquer um novo colaborador sem antes ter preenchido todos os requisitos do Departamento de Recursos Humanos.

O acesso concedido a um usuário deve passar por um processo de revisão a cada 12 (doze) meses, a fim de detectar concessões desnecessárias. Quaisquer alterações nas atividades e tarefas realizadas requerem reavaliação dos direitos e privilégios de acesso concedidos com a atualização do Termo de Compromisso e Responsabilidade sobre o Uso de Recursos de Informática. A revisão

anual é responsabilidade do gerente responsável pelo usuário e o controle dessa revisão é de responsabilidade do Setor de Tecnologia da Informação.

Quando da liberação de acesso lógico para colaboradores (terceiros), o Setor de Tecnologia da Informação deve cadastrar o acesso dos mesmos com data de expiração vinculada à vigência do contrato. O Gestor do Usuário terceiro é o responsável por esta informação.

A capacidade de acesso a determinado sistema não implica na autorização de uso deste, ou seja, tudo que não possui permissão explícita de uso é implicitamente fechado.

Cabe ao Departamento de Recursos Humanos informar imediatamente o setor de Tecnologia da Informação quando do desligamento de funcionários. Cabe ao Setor de Tecnologia da Informação desautorizar o acesso do usuário desligado aos sistemas da Cooperativa Vinícola Aurora Ltda imediatamente após a comunicação do Departamento de Recursos Humanos. Esse procedimento ocorre com abertura de chamado técnico no Service Desk.

Cabe ao responsável pela empresa terceira informar ao gestor do contrato quando ocorrem desligamentos ou substituições de pessoal na equipe que presta serviços à Cooperativa Vinícola Aurora Ltda.

Cabe ao gestor responsável pelos contratos de colaboradores (terceiros) desligados informar imediatamente os gestores da informação e dos recursos concedidos ao colaborador em questão para que seu acesso seja revogado.

Quando do seu desligamento, os usuários comprometem-se a devolver à Cooperativa Vinícola Aurora Ltda todas informações confidenciais e internas sob sua posse.

Ao usuário não se reserva o direito da posse de informações confidenciais e internas da organização após seu desligamento.

Os usuários são diretamente responsáveis por todas as atividades associadas e utilização de senha pessoal. Usuários devem alterar sua senha pessoal quando houver suspeita de interceptação ou uso indevido. Esta suspeita deve ser informada ao Setor de Tecnologia da Informação, o qual informará todos os procedimentos necessários.

Situações de acesso não autorizadas serão identificadas pelo Setor de Tecnologia da Informação e repassadas para o Departamento de Recursos Humanos, podendo ser motivo de sanções previstas pela empresa.

O usuário que realizar um período de férias ou ausência deve ter seus acessos físicos e lógicos suspensos pelo período relativo, exceto cargos de confiança. Assim que o usuário retornar às suas atividades, o restabelecimento de seus privilégios deve ser solicitado pela gerência responsável pelo usuário ao Setor de Tecnologia da Informação.

Todos os arquivos de trabalho devem ser mantidos na pasta da rede designada para cada departamento.

Informação ou arquivos particulares não devem ser mantidos na infraestrutura da Vinícola Aurora (pastas no computador local ou pasta da rede). A Vinícola Aurora não se responsabiliza por arquivos particulares armazenados na sua infraestrutura. O usuário não deve criar expectativa de privacidade caso disponibilize informações particulares, em desacordo com esta política.

O setor de Tecnologia da Informação possui a liberalidade de excluir arquivos encontrados na estrutura da Vinícola Aurora que não possuam relação com as atividades da mesma.

8.3. Confidencialidade de Informações

Todas as pessoas ou outras entidades (Colaboradores e Terceiros/Parceiros) que obtiverem acesso a informações confidenciais e internas da Cooperativa Vinícola Aurora Ltda devem aceitar formalmente as determinações do “Termo de Acordo de Confidencialidade e Não Divulgação de Informações”.

8.4. Gerenciamento da Segurança em Redes

A conexão de computadores ou redes de terceiros à rede interna da Cooperativa Vinícola Aurora Ltda somente deve ser realizada após aprovação do Setor de Tecnologia da Informação através de seu gestor ou alguém designado pelo mesmo.

Equipamentos de terceiros somente poderão conectar-se à rede ou recursos da Cooperativa Vinícola Aurora Ltda se atendidos os requisitos impostos pelo Setor de Tecnologia da Informação.

A Cooperativa Vinícola Aurora Ltda se reserva ao direito de auditar tais equipamentos para garantia de segurança de seus sistemas de informação. Requisitos como: Deve prover autenticação dos usuários, haver backup das configurações dos ativos de rede, Registro de acesso dos administradores dos ativos, Autenticação, Encriptação, Controle de acessos, etc.

A conexão de computadores e redes internas com redes públicas somente poderá ser realizada mediante aprovação do Setor de Tecnologia da Informação e aplicação dos controles de segurança adequados.

8.5. Alterações em Configurações

Os usuários são proibidos de instalar novos sistemas nos computadores ou demais dispositivos de hardware.

Quando da necessidade de alterações na configuração de sistemas, o usuário deve requisitar ao Setor de Tecnologia da Informação, sujeito à autorização da gerência responsável e aprovação do Setor de Tecnologia da Informação.

Os usuários devem utilizar somente os sistemas e recursos disponibilizados pela Cooperativa Vinícola Aurora Ltda. A utilização de softwares, sistemas ou equipamentos particulares devem ser avaliados pelo Setor de Tecnologia da Informação.

8.6. Uso de Internet

O acesso à Internet e seus serviços devem ser restritos a atividades relacionadas com os interesses da organização, respeitando o Regulamento de Uso da Internet, Correio Eletrônico e Outros da Cooperativa Vinícola Aurora Ltda.

As informações obtidas através da Internet e seus serviços devem ser considerados, em princípio, não confiáveis. As diversas informações como, por exemplo, endereços de remetentes, informações financeiras, avisos de segurança, devem ser confirmados antes de serem considerados confiáveis.

Usuários não devem participar de serviços e grupos de discussão e semelhantes como, por exemplo, fóruns, salas de conversação, listas de correio eletrônico, redes de mensagens instantâneas, salvo exceções formalmente autorizadas pela gerência responsável e comunicadas ao Setor de Tecnologia da Informação.

A Cooperativa Vinícola Aurora Ltda se reserva ao direito de remover quaisquer informações publicadas em grupos de discussão que possam vir a prejudicar a Cooperativa Vinícola Aurora Ltda, seus clientes, parceiros de negócio e demais entidades relacionadas.

Transferências de arquivos da Internet (Upload /Download de dados) que não estejam ligados aos interesses da organização são proibidas aos usuários. Quando houver necessidade de transferência de arquivos, o solicitante deve se reportar ao Setor Tecnologia da Informação.

A transferência de informações a outros países deve ser prévia e formalmente autorizada pelo Gestor da Área. Alguns países possuem normas rígidas sobre a transferência de informações como, por exemplo, arquivos pessoais, informações privativas de clientes e etc.

Demais utilizações da Internet não listadas neste documento, que existam ou venham a ser criadas, devem ser solicitadas à gerência responsável. Se essa utilização for considerada pelo gerente como adequada ao Regulamento de Uso da Internet, Correio Eletrônico e Outros e de interesse da organização, deve ser encaminhada ao Setor de Tecnologia da Informação, para análise, aprovação e disponibilização.

O usuário será responsabilizado pelos atos e acessos indevidos, conforme sanções previstas pela empresa.

8.7. Uso de Correio Eletrônico

O correio eletrônico é considerado recurso da Cooperativa Vinícola Aurora Ltda, devendo ser utilizado para atividades de interesse da organização e respeitando o Regulamento de Uso da Internet, Correio Eletrônico e Outros da empresa.

Os usuários não devem compartilhar contas de correio eletrônico, estando seu uso diretamente associado ao usuário proprietário.

O repasse automático de mensagens de uma conta à outra deve ser aprovado pela gerência responsável e solicitado ao Setor de Tecnologia da Informação.

Os usuários têm permissão de repassar para endereços externos à Cooperativa Vinícola Aurora Ltda apenas mensagens que contenham informações classificadas como públicas. Informações classificadas como confidencial ou uso interno somente poderão ser transmitidas externamente após aprovação do Setor de Tecnologia da informação e atendimento dos requisitos de segurança impostos.

São proibidas mensagens profanas, obscenas, indecentes, lascivas, materiais que explícita ou implicitamente se refiram à conduta sexual, incitações raciais, que constituam apologia ao fanatismo, demais conteúdos ilegais ou que possam de alguma forma ofender demais pessoas. Também é proibida a utilização do correio eletrônico para exercer o direito de liberdade de expressão.

O usuário será responsabilizado pelos atos e acessos indevidos, conforme sanções previstas no Regulamento de Uso da Internet, Correio Eletrônico e Outros

Endereços de correio eletrônico corporativos são informações classificadas como Uso Interno, sua divulgação deve ser restrita. O objetivo desta medida é evitar que os colaboradores sejam alvo de propaganda eletrônica, “spamming”, entre outras práticas prejudiciais ao ambiente da empresa.

8.8. Uso de Dispositivos Móveis

O uso, manuseio ou custódia de equipamentos portáteis da Cooperativa Vinícola Aurora Ltda somente é permitido após aprovação do Setor de Tecnologia da Informação através do “Termo de Responsabilidade e Uso de Dispositivos Móveis” e do cumprimento dos requerimentos de segurança solicitados.

Exemplos de equipamentos portáteis são: notebooks, celulares, entre outros. Proteções devem ser estabelecidas para evitar acessos não autorizados e/ou a divulgação das informações armazenadas nos dispositivos. Deve-se também considerar o cenário de BYOD da empresa.

8.9. Uso de Sistemas Telefônicos

O uso de sistemas telefônicos é monitorado, permitindo a identificação das chamadas.

Números de telefone e ramais internos são informações classificadas como Uso Interno, sua divulgação deve ser restrita.

8.10. Vírus de Computador

Todos os sistemas suscetíveis à contaminação por vírus de computador devem possuir sistema antivírus instalado e ativo.

Todos os arquivos recebidos devem ser automaticamente verificados quanto à contaminação por vírus antes de sua execução ou utilização.

Os usuários que receberem alertas de contaminação de vírus em sua estação de trabalho, ou quando houver suspeita de contaminação, devem cessar sua atividade e comunicar o Setor de Tecnologia da Informação imediatamente.

Os usuários não devem remover, apagar, limpar arquivos infectados ou executar qualquer atividade de combate a um vírus de computador.

Os usuários são proibidos de armazenar ou desenvolver vírus de computador ou código malicioso.

8.11. Backup de Dados / Cópias de Segurança

Todas as informações relativas às rotinas de backup de dados estão contidas no documento "Sistemática de backups".

8.12. Uso de Telefones Celulares

O uso, manuseio ou custódia de equipamentos celulares de propriedade da Cooperativa Vinícola Aurora Ltda é permitido somente mediante aprovação do Departamento de Recursos Humanos e atendimento aos requisitos de segurança determinados no formulário “Termo de Responsabilidade e Uso de Dispositivos Móveis”.

8.13. Uso de Programas de Computador

Todos os programas e sistemas de informação devem ser utilizados para propósitos de interesse da organização, respeitando o Termo de Compromisso e Responsabilidade sobre o uso de Recursos de Informática e outros.

Controlar todos os softwares que necessitam de licenciamento, sendo devidamente atualizados e licenciados,

Programas e sistemas que não são utilizados ou não fazem parte dos programas homologados pela Cooperativa Vinícola Aurora Ltda devem ser desinstalados.

É permitida apenas a utilização de programas homologados pelo Setor de Tecnologia da Informação e o armazenamento de informações condizentes com interesses da Cooperativa Vinícola Aurora Ltda.

A lista de softwares homologada pela Cooperativa Vinícola Aurora Ltda é controlada e atualizada pelo Setor de Tecnologia da Informação.

8.14. Uso de Criptografia

Os usuários devem utilizar somente mecanismos de criptografia homologados pelo Setor de Tecnologia da Informação.

8.15. Trabalho Remoto

O acesso remoto a informações da Cooperativa Vinícola Aurora Ltda somente é permitido quando houver necessidade do exercício de atividades de interesse da organização.

A conexão externa aos sistemas internos da Cooperativa Vinícola Aurora Ltda deve ser formalmente autorizada pelo gestor da área do sistema que será acessada e aprovada pelo Setor de Tecnologia da Informação.

A Cooperativa Vinícola Aurora Ltda se reserva ao direito de auditar tais equipamentos periodicamente a fim de garantir a segurança das informações manipuladas. Os equipamentos a princípio devem ter acesso restringido de familiares ou visitantes às informações e ao próprio equipamento.

8.16. Desenvolvimento de Sistemas

Os usuários não devem desenvolver qualquer tipo de programa de computador, no todo ou em partes. Esta tarefa é exclusiva dos analistas de sistemas e programadores autorizados pelo Setor de Tecnologia da Informação.

Recursos de sistemas de escritório como, por exemplo, fórmulas de cálculo e macros não são considerados programas de computador, estando os usuários permitidos a utilizar, desde que sejam temas de trabalho e tenham seu backup em rede corporativa.

8.17. Descarte de Equipamentos

A necessidade do descarte de equipamentos de informática e telecomunicações deve ser comunicada ao Setor de Tecnologia da Informação. O Setor de Tecnologia da Informação deve garantir que todas as informações contidas nos equipamentos sejam salvas e após destruídas de forma segura

8.18. Registros de Eventos e Monitoramento

Todas as atividades, ações e a utilização de recursos de Tecnologia da Informação da Cooperativa Vinícola Aurora Ltda, como, por exemplo, Internet e correio eletrônico estão sujeitas à monitoração, gravação, armazenamento e verificação.

Tais atividades estão sujeitas à análise quando da suspeita da realização de atividades não autorizadas ou do não cumprimento das determinações previstas pela empresa.

A Cooperativa Vinícola Aurora Ltda se compromete a não analisar informações pessoais enquanto não houver suspeita ou evidência da realização de atividades não autorizadas.

8.19. Direitos de Propriedade Intelectual

A Cooperativa Vinícola Aurora Ltda é a proprietária legal de todas as informações criadas através de seus recursos. Todas as informações incluindo patentes e invenções desenvolvidas por usuários mantenedores de vínculo contratual com a Cooperativa Vinícola Aurora Ltda são de propriedade da organização.

Todas as informações manipuladas pela Cooperativa Vinícola Aurora Ltda devem seguir o "Termo de Cessão de Direitos Relacionados à Propriedade Intelectual".

8.20. Licença de Softwares

Os usuários somente devem utilizar softwares licenciados e fornecidos pela Cooperativa Vinícola Aurora Ltda. A utilização de softwares não licenciados é proibida e constitui crime de pirataria.

Não devem ser mantidas cópias de softwares de propriedade da Cooperativa Vinícola Aurora Ltda, a menos que formalmente autorizado pelo desenvolvedor ou fornecedor do sistema e aprovado pelo Setor de Tecnologia da Informação.

Todos os softwares e demais produtos adquiridos devem ter sua compra e utilização registradas junto ao fabricante ou desenvolvedor.

O Setor de Tecnologia da Informação se reserva ao direito de remover quaisquer softwares ou sistemas não homologados ou não licenciados instalados nos equipamentos e demais recursos aplicáveis, sem aviso prévio.

8.21. Relações com terceiros na cadeia de suprimentos

Todas as informações de terceiros que estejam sob custódia da Cooperativa Vinícola Aurora Ltda devem ser classificadas e a utilização adequada.

A divulgação ou repasse de informações confidenciais e internas ou sistemas internos a terceiros é restrita a processos de negócio e atividades de trabalho.

Tais divulgações ou repasses devem ser realizados com a garantia formal de atendimento dos mesmos requisitos de segurança utilizados na Cooperativa Vinícola Aurora Ltda. A divulgação ou repasse de informações confidenciais e internas ou sistemas internos deve ser autorizada pelo gestor da área.

8.22. Uso da Marca

A utilização de marcas pertencentes a Cooperativa Vinícola Aurora Ltda é restrita a propósitos de negócio. Esta utilização deve ser formalmente autorizada pela direção da empresa.

A utilização por terceiros do nome ou logomarca Cooperativa Vinícola Aurora Ltda, bem como demais nomes ou logomarcas pertencentes à Cooperativa Vinícola Aurora Ltda sem autorização legal da organização, é proibida. Deve ser seguido os preceitos do "Termo de Cessão de Direitos Relacionados à Propriedade Intelectual".

8.23. Gestor da Informação da Política de Segurança da Informação

A diretoria da Cooperativa Vinícola Aurora Ltda é a responsável pela Política de Segurança da Informação. Qualquer consideração acerca deste conjunto de documentos deve ser enviada ao e-mail segurancadainformacao@vinicolaaurora.com.br

Questões não abordadas na Política de Segurança da Informação devem ser avaliadas e decididas pela gerência responsável pelo usuário, sob aprovação do Setor de Tecnologia da informação ou recurso em questão.

Estas questões devem sempre ser encaminhadas ao Comitê Gestor da Segurança da Informação formado por integrantes do setor de tecnologia da informação.

8.24. Direitos, Deveres e Sanções

O usuário estará sujeito a seguir estritamente as orientações contidas nesta Política de Segurança da Informação, sob pena de advertência.

Violações das determinações desta política e arquivos referenciados podem levar a sanções disciplinares segundo critérios estabelecidos pelo "Código de Conduta" da Cooperativa Vinícola Aurora Ltda e pelo Departamento de Recursos Humanos.

No caso de Terceiros, violações da política podem causar o cancelamento do contrato de prestação de serviços. Eventual dano material ou moral causado a Cooperativa Vinícola Aurora Ltda ou a terceiros é passível de indenização pelo responsável.

8.25. Segregação de Funções

Funções conflitantes e áreas de responsabilidade devem ser segregadas (separadas) para reduzir as oportunidades de modificação não autorizada ou não intencional, ou uso indevido dos ativos da organização.

Destina-se a mitigar as oportunidades de qualquer pessoa estar em posição de ocultar erros ou fraudes no curso normal de suas funções.

8.26. Segregação de Redes

Grupos de serviços de informação, usuários e sistemas de informação devem ser segregados em redes físicas ou virtuais. Dessa forma eventos pontuais não irão afetar todos os sistemas da organização.

8.27. Gestão de Ativos

Os ativos associados com informação e com os recursos e processamento da informação devem ser identificados e um inventário destes ativos deve ser estruturado e mantido.

Todos os funcionários e partes externas devem devolver todos os ativos da organização que estejam em sua posse após o encerramento de suas atividades, do contrato ou acordo.

8.28. Segurança em Recursos Humanos

Verificações do histórico devem ser realizadas para todos os candidatos a emprego, de acordo com a ética, regulamentações e leis relevantes, e deve ser proporcional aos requisitos do negócio, aos riscos percebidos e a classificação das informações a serem acessadas.

Antes da Contratação
Assegurar que funcionários e partes externas entendam suas responsabilidades e estão em conformidade com os papéis para os quais eles foram selecionados.

Durante a Contratação
Assegurar que os funcionários e partes externas estão conscientes e cumprem as suas responsabilidades pela segurança da informação.

Encerramento e Mudança da Contratação
Proteger os interesses da organização como parte do processo de mudança ou encerramento da contratação.

8.29. Contato com Autoridades

Contato com autoridades relevantes devem ser mantidos. Manter tais contatos é um requisito para apoiar incidentes de segurança da informação. Esses incluem serviços de emergência como: Hospitais, Ambulâncias, Bombeiros, Polícias, Fornecedores de Telecomunicações, ANPD, etc.

8.30. Segurança da Informação em Gerenciamento de Projetos

A segurança da informação deve ser considerada no gerenciamento de projetos. Riscos de segurança da informação devem ser identificados e considerados como parte de um projeto. Se aplica a qualquer tipo de projeto, independente do seu propósito.

8.31. Segurança Física e dos Ambientes

Prevenir o acesso físico não autorizado, danos e interferências com os recursos de processamento de informações. Perímetros de segurança devem ser identificados em áreas que contenham informações críticas.

Controle por biometria é utilizado para acesso aos datacenters. Somente pessoas autorizadas têm permissão de entrada.

8.32. Proteção contra Ameaças Externas e Meio Ambiente

Projetada e aplicada a proteção física contra desastres naturais, maliciosos ou acidentais. Entende-se como: Fogo, Inundação, Terremoto, Explosão, Manifestações Civis e outras formas de desastre natural ou provocados.

8.33. Segurança do Cabeamento

Os cabeamentos de energia e telecomunicações que dão suporte aos serviços de informações devem ser protegidos contra interceptação, interferência e danos.

8.34. Manutenção de Equipamentos

Prover a manutenção preventiva, preditiva e corretiva de equipamentos para manter sua integridade e disponibilidade.

8.35. Remoção de Ativos

Equipamentos e informações não devem ser retirados do local sem autorização prévia e controle.

8.36. Mesa Limpa e Tela Limpa

Documentos sensíveis ou confidenciais impressos devem ser guardados em local seguro quando não em uso ou quando o escritório estiver desocupado. É importante manter a posição de trabalho organizada.

Usuários devem bloquear a estação de trabalho que estiverem utilizando quando interromperem, mesmo que por breves momentos, suas atividades. É responsabilidade do usuário garantir o bloqueio ou liberação do equipamento para utilização por outros usuários.

8.37. Segurança nas Operações

Procedimentos Operacionais Padrão devem ser documentados e disponibilizados a todos os usuários que necessitem dos mesmos.

Esses procedimentos devem estar associados a recursos de processamento da comunicação e informação.

8.38. Segurança da Informação na Gestão de Mudanças

Devem ser controladas mudanças na organização e nos recursos de processamento que afetam a segurança da informação.
Documentos de mudança com informações relevantes para a manutenção da segurança da informação devem ser utilizados em todas as mudanças.

8.39. Gestão da Capacidade

A utilização de recursos deve ser monitorada e ajustada. Projeções futuras devem ser feitas visando garantir a disponibilidade dos sistemas.
A criticidade do negócio deve ser considerada nos ajustes de monitoramento e capacidade.

8.40. Proteção contra Malware

Controles de detecção, prevenção e recuperação para proteger contra Malware devem ser implementados, combinados com um programa de conscientização dos usuários. Monitoramento e combate feito via Antivírus BitDefender, ações e tomada de decisões analisadas em conjunto entre equipe interna e terceirizada.

8.41. Sincronização dos Relógios (NTP)

Os relógios de todos os sistemas de processamento de informações relevantes devem estar sincronizados com uma fonte única de tempo e precisa.

8.42. Segurança dos Serviços de Redes

Mecanismos de segurança, níveis de serviço e requisitos dos serviços de rede devem ser identificados e incluídos nos acordos de nível de serviço.

8.43. Gestão de Incidentes de Segurança da Informação

Assegurar um enfoque consistente e efetivo para gerenciar os incidentes de segurança da informação, incluindo a comunicação de fragilidades e potenciais eventos.

Quaisquer incidentes identificados que possam afetar a segurança da informação devem ser imediatamente informados ao Comitê Gestor da segurança através do E-mail: segurancadainformacao@vinicolaaurora.com.br

Nos casos de incidente de violação de dados pessoais, além das diretrizes aqui contidas, as diretrizes contidas na Norma de Gestão de Incidentes de Segurança da Informação e na Política Geral de Proteção de Dados Pessoais deverão ser observadas.

8.44. Continuidade da Segurança da Informação

Requisitos de segurança de um PCN ou DR devem contemplar a continuidade da segurança da informação.

8.45. Redundâncias

Os recursos de processamento de informações devem ser providos de redundância lógica e elétrica.

8.46. Proteção de Registros

Convém que registros sejam protegidos contra perda, destruição, falsificação, acesso e liberação não autorizado, cumprindo os requisitos regulamentares, estatutários, contratuais e do negócio.

8.47. Proteção e Privacidade de Informações de Identificação Pessoal

Convém que todos os requisitos da LGPD sejam atendidos na sua íntegra.

8.48. Análise Crítica da Segurança da Informação

Assegurar que a segurança da informação esteja implantada e operada de acordo com as políticas e procedimentos da organização. Auditoria interna ou externa deve ser realizada para certificar a PSI existente.

8.49. Conscientização, Educação e Treinamento em Segurança da Informação

Realizar treinamentos com todos os funcionários visando a conscientização sobre segurança da informação.

9. Papéis e responsabilidades

Cabe a todos os colaboradores, diretores, gestores, estagiários e prestadores de serviços cumprir fielmente a Política de Segurança da Informação buscar orientação em caso de dúvidas relacionadas à segurança da informação; proteger as informações contra acesso, modificação, destruição ou divulgação não-autorizados; assegurar que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades aprovadas pela Vinícola Aurora; cumprir as leis e as normas aplicáveis; e comunicar imediatamente a quando do descumprimento ou violação desta política.

9.1. Alta direção da Vinícola Aurora

É responsabilidade da Alta Direção:

- Aprovar a Política de Segurança da Informação e suas revisões;
- Assegurar que a Política de Segurança da Informação e os objetivos de segurança da informação estejam estabelecidos e compatíveis com a direção estratégica da organização;
- Garantir que os recursos necessários para o sistema de gestão da Segurança estejam disponíveis.

9.2. Comitê Gestor da Segurança da Informação (CGSI)

Fica constituído o Comite Gestor de Segurança da Informação, contando com a participação de, pelo menos, um representante da diretoria e um membro sênior das seguintes áreas: Tecnologia da Informação, Segurança da Informação, Recursos Humanos, Jurídico.

É responsabilidade do CGSI:

- Redigir e promover melhorias e revisões nas políticas de Segurança da Informação e procedimentos relacionados;
- Aprovar os processos, políticas, normas e procedimentos derivados da Política de Segurança da Informação;
- Analisar os casos de irregularidade ou violação das políticas de Segurança da Informação e, quando for o caso, encaminhá-los à Alta direção;
- Garantir a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;
- Garantir que as atividades de segurança da informação sejam executadas em conformidade com a Politica de Segurança da Informação;
- Propor projetos e iniciativas relacionadas à melhoria da Segurança da Informação da Vinícola Aurora;
- Promover a divulgação da Política de Segurança da Informação e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da Vinícola Aurora;
- Promover treinamentos e orientações sobre as políticas e procedimentos de Segurança da Informação.

9.3. Gestor da Segurança da Informação

É responsabilidade do Gestor de Segurança da Informação:

- Convocar e coordenar as reuniões do Comitê Gestor da Segurança da Informação;
- Apoiar o Comitê Gestor da Segurança da Informação em suas deliberações;
- Elaborar e propor ao Comitê Gestor da Segurança da Informação as normas e procedimentos de segurança da informação, necessários para se fazer cumprir esta política;
- Receber e avaliar projetos relacionados ao aperfeiçoamento da Segurança da Informação;
- Conduzir a gestão e operação da segurança da informação, tendo como base esta política;
- Gerenciar os riscos de Segurança da Informação;
- Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado de acordo com a Norma de Gestão de Incidentes e Violação de Dados Pessoais.

9.4. Equipe de Infraestrutura e Segurança da Informação

É responsabilidade da equipe de Infraestrutura e Segurança da Informação:

- Manter o ambiente tecnológico estável, operacional, atualizado, íntegro, disponível e monitorado;
- Elaborar e atualizar os procedimentos relativos à operacionalidade do ambiente tecnológico;
- Instalar e configurar os ativos de software e hardware necessários à operacionalidade do ambiente tecnológico;
- Implementar mecanismos de segurança com base no valor associado às informações e ao impacto oriundo da perda dessas informações;
- Promover instrução relacionada à Segurança da Informação;
- Acompanhar e analisar as transações e alterações relacionadas à Segurança da Informação, para fins de rastreamento e auditoria;
- Realizar, periodicamente, monitoramento e auditoria de segurança no ambiente tecnológico;
- Monitorar o ambiente computacional e priorizar medidas preventivas, em detrimento de controles reativos.

9.5. Gestores de usuários

É responsabilidade dos Gestores de Usuários:

- Ser referência quanto à Segurança da Informação;
- Garantir que as diretrizes e os aspectos aqui definidos sejam seguidos;
- Assegurar que as suas equipes tenham conhecimento das políticas e dos procedimentos de Segurança da Informação;
- Ao requisitar a concessão de acesso físico ou lógico, sempre optar por conceder somente aquilo que seja necessário para execução da função;
- Contribuir para a melhoria dos processos e procedimentos sob sua
- responsabilidade para que atendam às políticas de Segurança da Informação;
- Gerenciar os acessos dos usuários terceiros informando imediatamente o desligamento para o Setor de Tecnologia da Informação.

9.6. Colaboradores e prestadores de serviços

É responsabilidade dos Colaboradores e prestadores de serviços:

- Ler, compreender e cumprir integralmente os termos da Política de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
- Ser responsável pelo uso adequado e seguro dos ativos de informação e das informações a que tenha acesso;

- Buscar orientação sempre que não estiver absolutamente seguro quanto ao manuseio das informações;
- Comunicar à Comitê Gestor da Segurança da Informação qualquer evento que viole esta política ou coloque ou possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da Vinícola Aurora;
- Responder pela inobservância da Política de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.

9.7. Gestores da informação

É responsabilidade dos Gestores de Informação:

- Autorizar o acesso às informações que são de sua responsabilidade;
- Designar a categoria de classificação de todas as informações sob sua responsabilidade;
- Revisar periodicamente os perfis de acesso de acordo com esta política.

10. Gestão da política

10.1. Esta política é aprovada pela Alta direção da Vinícola Aurora, passando a ser amplamente aplicada na data de sua publicação.

10.2. A cada 12 meses, ou antes deste prazo a critério do Comitê Gestor da Segurança da Informação, esta política será revisada para garantir sua contínua pertinência e adequação as necessidades da Cooperativa Vinícola Aurora.