POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – CAPEBE

INTRODUÇÃO

A Política de Segurança da Informação – PSI, é o documento que orienta e estabelece critérios e diretivas cooperativas do **Cooperativa Agropecuária de Boa Esperança - CAPEBE** para a proteção dos ativos de informações e responsabilidade legal para todos os colaboradores, devendo, portanto, ser aplicada a todas as áreas da cooperativa.

A presente política está embasada na família ABNT ISO/IEC 27000, reconhecida por abordar conceitos, códigos de conduta e práticas no que concerne à segurança da informação e na Lei 13.709/2018 – Lei Geral de Proteção de Dados, além das demais leis aplicáveis.

OBJETIVOS

A presente política tem por objetivo estabelecer critérios e diretrizes para os colaboradores da **CAPEBE** seguirem padrões comportamentais para garantir a segurança dos ativos de informações no exercício laboral, de forma a atender todas as necessidades do negócio e a proteção legal da empresa e também do indivíduo.

Preservar as informações do **CAPEBE** quanto a:

- **Integridade:** Garantia de que os ativos de informação da **CAPEBE** contenham, em seu conteúdo, inalterabilidade indevidas ou ilícitas, protegendo-os em seu armazenamento ou transmissão [ISO/IEC 13335-1:2004].
- **Confidencialidade:** Garantia de que a informação da **CAPEBE** não esteja disponível, ou seja revelada a indivíduos, a entidades ou processos não autorizados [ISO/IEC 13335-1:2004].
- **Disponibilidade:** Garantia de que a informação da **CAPEBE** esteja acessível e utilizável sempre que houver demanda e necessidade por colaborador autorizado [ISO/IEC 13335-1:2004].

TERMOS E DEFINIÇÕES

Para que haja um melhor entendimento desta política, os termos utilizados na elaboração desta serão conceituados a seguir com base nas definições elencadas pela ISO/IEC 27001:

1. **Ativo:** qualquer coisa que tenha valor para a organização [ISO/IEC 13335-1:2004];
2. **Segurança da informação:** preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas [ABNT NBR ISO/IEC 17799:2005];
3. **Evento:** Acontecimento que acarrete na mudança do estado atual de um processo;
4. **Evento de segurança da informação:** uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação [ISO/IEC TR 18044:2004];
5. **Incidente de segurança da informação**: um simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação [ISO/IEC TR 18044:2004];
6. **Risco:** Combinação da probabilidade de ocorrência de um evento e seus respectivos impactos;
7. ***Malwares*:** O nome *malware* vem do inglês *malicious software* (programa malicioso). Refere-se a qualquer tipo de programa indesejado, instalado sem seu consentimento e que pode trazer danos ao computador;
8. **SPAM:** É o termo usado para referir-se a e-mails não solicitados, que geralmente são enviados para um grande número de pessoas;
9. ***Phishing:*** Mensagens de e-mail que solicitam dados do usuário de forma direta ou através de redirecionamentos para sites ou números de telefone, a fim de roubar sua identidade;

10. ***Mail bombing:*** Envio de mensagens eletrônicas em massa para um determinado destinatário com o objetivo de sobrecarregar o serviço de e-mail e torná-lo inutilizável ou indisponível;

APLICAÇÃO DA PSI

As diretrizes aqui apresentadas devem ser seguidas por todos os colaboradores, coordenadores e diretores da **CAPEBE.**

Esta política dá ciência a cada colaborador, coordenador e diretores de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, sendo armazenados com a finalidade de garantir a defesa da **CAPEBE** em processos judiciais, administrativos ou arbitrais, além de garantir o exercício de interesses legítimos da cooperativa ou de terceiros.

É também obrigação de cada colaborador se manter atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

DIRETRIZES DA PSI

A presente Política adotará algumas diretrizes como base norteadora para a sua elaboração, sendo as seguintes:

1. **Informação como patrimônio:** Toda informação produzida ou recebida pelos colaboradores como resultado da atividade profissional contratada pela **CAPEBE** pertence a cooperativa. As exceções devem ser explícitas e formalizadas em contrato entre as partes.
2. **Acesso à informação Controlado:** Toda a informação produzida pelos colaboradores da **CAPEBE,** bem como aquelas recebidas em função do exercício da atividade profissional da cooperativa, será devidamente monitorada para resguardar o seu acesso somente por pessoas que detenham expressa autorização para tal, de acordo com a classificação da informação.

3. **Incidentes de Seguranças devidamente tratados:** Qualquer incidente de segurança da informação será devidamente publicado, apurado e tratado pela **CAPEBE.**
4. **A CAPEBE deve monitorar os seus ativos:** A **CAPEBE** poderá registrar todo o uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.
5. **Auditar internamente o cumprimento da PSI:** A **CAPEBE** empregará todos os esforços necessários para fiscalizar o cumprimento interno desta política, bem como a sua manutenção.
6. **Responsabilidade e Comprometimento de TODOS:** O cumprimento desta política deverá ocorrer através do comprometimento de todos os colaboradores, coordenadores de área e diretores, sendo de responsabilidade de todos os integrantes da **CAPEBE** o seu cumprimento.
7. **Cuidado e Proteção com os equipamentos*:*** Os equipamentos de informática e comunicação, sistemas e informações são utilizados pelos colaboradores para a realização das atividades profissionais, e devem ser devidamente cuidados e conservados por estes. De forma excepcional, o uso pessoal dos recursos é permitido, desde que não prejudique o desempenho dos sistemas e serviços da cooperativa, tais como lentidão da internet, exposição da rede interna a riscos, utilização de material de papelaria em excesso e entre outros.

PRINCÍPIOS DA PSI

Toda a política de segurança da informação da **CAPEBE** será estruturada de forma a garantir a observância dos seguintes princípios: *(i)* promoção de um ambiente de segurança para os colaboradores, coordenadores, diretores, cooperados e clientes; *(ii)* implementação de cultura de proteção de ativos informacionais entre os colaboradores, coordenadores e diretores assegurando a segurança da informação; e *(iii)* manutenção da conformidade da **CAPEBE** com as normas brasileiras que regem o uso da internet e proteção de dados, além das normas internacionais de Segurança da Informação.

REQUISITOS DA PSI

Para que a presente política seja devidamente implementada na **CAPEBE,** deverão ser observados requisitos específicos e adotados novos procedimentos.

Desta maneira, esta política deverá ser comunicada a todos os estagiários, colaboradores, coordenadores e diretores, sendo disponibilizada a todos de forma facilitada e gratuita.

Esta política também deverá ser implementada através de um Comitê Multidisciplinar de *Compliance* e Privacidade, para gestão e implementação, sendo formado essencialmente por colaboradores de diversos setores da **CAPEBE,** sendo revista e atualizada periodicamente, sempre que houver algum fato relevante ou evento que motive sua revisão antecipada, conforme análise e decisão do supracitado Comitê.

Para além, esta política deverá constar em todos os contratos da **CAPEBE** através de acordo de confidencialidade ou cláusula de confidencialidade, como condição imprescindível para que possam ser concedidos acessos aos ativos de informação disponibilizados pelos clientes ou disponibilizados pela cooperativa.

A presente política deverá ser comunicada a todos os colaboradores, prestadores de serviço, menores aprendizes e estagiários na fase de contratação, sendo estes devidamente orientados sobre todas as normas e procedimentos de segurança, bem como correto uso dos ativos e equipamentos disponibilizados pela **CAPEBE,** tendo por objetivo a redução de possíveis riscos. Os colaboradores, menores aprendizes e estagiários deverão assinar termo de responsabilidade.

Todo e qualquer incidente que afete a segurança da informação deverá ser imediatamente comunicado ao Encarregado da **CAPEBE,** este deverá adotar as medidas cabíveis, com base na legislação pátria e nas normas editadas nesta política.

Assim, para implementação desta política também é necessário a elaboração de plano de contingência e continuidade dos principais sistemas e serviços, sendo testados anualmente, para reduzir qualquer risco de perda de confidencialidade, integridade e disponibilidade dos ativos de informação.

Esta PSI deverá ser implementada na **CAPEBE** por meio de procedimentos específicos, obrigatórios para todos os colaboradores, independentemente do nível

hierárquico ou função na empresa, bem como de vínculo empregatício ou prestação de serviço.

CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações devem ser classificadas e identificadas por rótulos, considerando os níveis: pública, interna, confidencial e confidencial restrita, respeitando o disposto na Política de Classificação de Ativos da Capebe.

RESPONSABILIDADES E ATRIBUIÇÕES

1. Colaboradores em Geral

Entende-se por colaborador toda e qualquer pessoa física, contratada CLT ou por meio de termo de estágio, contrato de menor aprendiz ou prestadora de serviço por intermédio de pessoa jurídica ou não, que exerça alguma atividade dentro ou fora da instituição.

Será de inteira responsabilidade de cada colaborador, todo prejuízo ou dano que vier a sofrer ou causar a **CAPEBE** e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas.

2. Coordenadores de Área e Gestores de Pessoas e/ou Processos

Ter postura exemplar em relação à segurança da informação, servindo como modelo de conduta para os colaboradores sob a sua gestão.

Atribuir aos colaboradores, na fase de contratação e de formalização dos contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento da PSI da **CAPEBE**.

Exigir dos colaboradores a assinatura do Termo de Compromisso e Ciência, assumindo o dever de seguir as normas estabelecidas, bem como se comprometendo a manter sigilo e confidencialidade, mesmo quando desligado, sobre todos os ativos de informações da **CAPEBE**.

Antes de conceder acesso às informações da instituição, exigir a assinatura do Acordo de Confidencialidade dos colaboradores casuais e prestadores de serviços que não estejam cobertos por um contrato existente, por exemplo, durante a fase de levantamento para apresentação de propostas comerciais.

Adaptar as normas, os processos, procedimentos e sistemas sob sua responsabilidade para atender a esta PSI.

3. Colaboradores Temporários (Regime de Exceção)

Os colaboradores em regime de exceção devem observar e cumprir rigorosamente o que está previsto nesta política. Podendo o Comitê Multidisciplinar constituído para aplicação desta PSI revogar a concessão de acessos a qualquer tempo, verificado o contexto da contratação, se esta não mais atender aos fins necessários ou se o colaborador estiver descumprimento as condições aqui definidas.

4. Setor de Tecnologia da Informação

Ao setor de tecnologia da informação da **CAPEBE** cabe a função de testar todos os controles utilizados para mitigação de risco e informar aos gestores os riscos residuais.

Aliado a isto, o setor de tecnologia da informação da **CAPEBE** é responsável por iniciar o processo interno de investigação e averiguação na ocorrência de incidentes de segurança da informação.

Configurar os equipamentos, ferramentas e sistemas concedidos aos colaboradores com todos os controles necessários para cumprir os requerimentos de segurança estabelecidos por esta PSI.

Os analistas integrantes do setor de Tecnologia da Informação da **CAPEBE** que possuam privilégios de usuários administradores e operadores dos sistemas utilizados pela cooperativa podem, em alguns casos, acessar arquivos e dados de outros usuários. Este acesso só será feito quando houver necessidade para execução de atividades operacionais sob sua responsabilidade, como por exemplo a manutenção dos computadores, a realização de cópias de segurança, auditorias ou testes no ambiente.

Ao setor de Tecnologia da Informação da cooperativa cabe a segregação de acessos lógicos, de acordo com a função de cada colaborador, a fim de mitigar os riscos de acesso dos colaboradores a funcionalidades e documentos não autorizados. Também é atribuída ao supracitado setor a responsabilidade pela fiscalização dos ativos informacionais que circulam na cooperativa (Pública, Interna, Confidencial e Confidencial estrita).

Gerar e manter as trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes. Para as trilhas geradas e/ou mantidas em meio eletrônico, implantar controles de integridade para torná-las juridicamente válidas como evidências.

Também, cabe ao setor de tecnologia da informação a implementação de controles que permitam a elaboração, implementação e manutenção de planos de contingência e continuidade, a fim de manter a disponibilidade dos ativos informacionais, bem como a sua integridade.

5. Cooperativa

A **CAPEBE** exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus colaboradores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis.

O não cumprimento dos requisitos previstos nesta PSI e das Normas de Segurança da Informação acarretará violação às regras internas da **CAPEBE** e sujeitará o usuário às medidas administrativas e legais cabíveis

ESTAÇÕES DE TRABALHO

As estações de trabalho devem ser mantidas de maneira a permitir que a sua estrutura permita a completa utilização pelo colaborador no seu trabalho, permanecendo operável para que os colaboradores não tenham suas atividades prejudicadas.

Devem ser adotadas as seguintes medidas de segurança:

1. O Colaborador deve zelar pelos equipamentos utilizados, mantendo-os em bom estado.
2. Não é permitido ao colaborador **PERSONALIZAR** os equipamentos, com adesivos, riscos, raspagem e a **RETIRADA DA ETIQUETA DE PATRIMÔNIO** do desktop;
3. É vedado aos colaboradores o **REPARO** de qualquer ferramenta de trabalho, principalmente as eletrônicas (computadores e etc.). Este deve informar o setor de infraestrutura da **CAPEBE**, para adoção das medidas necessárias;

4. Não é permitido ao colaborador, sem a prévia autorização da respectiva gestão, mudar os equipamentos eletrônicos e demais ferramentas de trabalho da sua estação de trabalho para outros locais.
5. O acesso das estações de trabalho somente se dará mediante **LOGIN E SENHA**;
6. É vedada a utilização de ferramentas **PESSOAIS** no ambiente da cooperativa, autorizado somente em casos excepcionais para o cumprimento de contrato de prestação de serviço em que seja extremamente necessário o uso de ferramenta pessoal para o desenvolvimento do trabalho. Ex: notebooks, tablets entre outros correlatos;
    a. A utilização de equipamentos pessoais como celulares e *smarthpones* é vedada e somente poderá ocorrer desde que haja autorização do gestor direto do setor do colaborador, cabendo a este gestor a averiguação do ambiente coorporativo para tal autorização, além da fiscalização do uso do aparelho.
7. É vedada a instalação de softwares ou sistemas pelos colaboradores, salvo aqueles que são classificados pelo sistema operacional como confiáveis. Este procedimento somente será realizado por analistas do setor de Tecnologia da Informação da cooperativa, devendo ser solicitado diretamente ao setor de Infraestrutura quando o software não possuir licença, que avaliará a segurança do programa e sua confiabilidade, aprovando ou não a solicitação;
8. Para os softwares que necessitam de licença, a solicitação deverá ser feita para os integrantes da diretoria e para o gerente do setor de Tecnologia da Informação, após a aprovação destes o analista de T.I da cooperativa realizará a instalação;
9. É vedada a instalação de softwares que **NÃO** possuam licença e não sejam homologados pelo setor de infraestrutura da cooperativa;
10. O Colaborador deverá fazer **LOGOFF** da estação de trabalho nos momentos em que se ausentar da mesma;
11. Da mesma maneira o colaborador deverá zelar pelos documentos impressos que ficarem na estação de trabalho na sua ausência, mantendo-os protegidos

e guardados em confirmado com a classificação da informação destes documentos;

12. Os documentos e arquivos relativos à atividade desempenhada pelo colaborador deverão, sempre que possível, serem armazenados em local próprio no servidor da rede, o qual possui rotinas de backup e controle de acesso adequado;
13. Documentos críticos e/ou confidenciais só podem ser armazenados no servidor da rede, nunca no disco local da máquina;
14. É vedado ao colaborador manter anotações de senhas, *logins*, informações confidenciais em blocos de notas, post its ou qualquer outro meio que facilite a obtenção da informação por terceiro não autorizado;
15. É proibido o uso de estações de trabalho para:

a. Tentar ou obter acesso não autorizado a outro computador, servidor ou rede;
b. Burlar quaisquer sistemas de segurança;
c. Interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
d. Cometer ou ser cúmplice de atos de violação, assédio sexual, perturbação, manipulação ou supressão de direitos autorais ou propriedades intelectuais sem a devida autorização legal do titular;
e. Hospedar pornografia, material racista, sexista, homofóbico ou qualquer outro que viole a legislação em vigor no país, a moral, os bons costumes e a ordem pública.

16. A infraestrutura da cooperativa não se responsabiliza por prestar manutenção ou instalar softwares em computadores que não sejam os da instituição;
17. As estações de trabalho são monitoradas por sistema próprio, o qual permite que seja identificada na rede. Desta forma, tudo que for executado na estação de trabalho é de responsabilidade do funcionário.

CORREIO ELETRÔNICO

O E-mail corporativo, principal forma de comunicação entre os colaboradores, é identificado como um ativo da cooperativa. Desta forma, se faz extremamente necessário que sejam adotadas medidas de segurança para utilização do correio

eletrônico, isto porque é através deste que ocorrem a maior parte da disseminação de *malwares*.

Assim, o objetivo desta norma é informar aos colaboradores da **CAPEBE** quais são as atividades permitidas e proibidas quanto ao uso do e-mail coorporativo. Desta forma, devem ser observadas as seguintes medidas:

1. O e-mail corporativo deve ser destinado a fins PROFISSIONAIS, relacionados as atividades dos colaboradores;
2. Os e-mails enviados ou recebidos de endereços EXTERNOS poderão ser monitorados pela CAPEBE, com o intuito de bloquear spams, malwares ou outros conteúdos maliciosos que violem a Política de Segurança da Informação;
3. O uso de e-mails pessoais é aceitável, se usado com moderação, em caso de necessidade e quando:
    a. Não contrariar as normas aqui estabelecidas;
    b. Não interferir, negativamente, nas atividades profissionais individuais ou na de outros colaboradores;
    c. Não interferir, negativamente, na CAPEBE e na sua imagem.
4. As mensagens de correio eletrônico sempre deverão incluir assinatura com o seguinte formato:
    a. Nome do colaborador;
    b. Gerência ou departamento;
    c. Nome da empresa;
    d. Telefone (s);
    e. Correio eletrônico.

Portanto, é proibido aos colaboradores o uso do correio eletrônico da **CAPEBE** para:

5. Enviar, com endereço eletrônico corporativo, mensagens com anúncios particulares, propagandas, vídeos, fotografias, músicas, mensagens do tipo “corrente”, campanhas ou promoções;
6. Abrir arquivos com origens desconhecidas anexados a mensagens eletrônicas;
7. Falsificar informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários;

8. Enviar qualquer mensagem por meios eletrônicos que torne seu remetente e/ou a **CAPEBE** ou suas unidades vulneráveis a ações civis ou criminais.
9. Enviar mensagens não solicitadas para múltiplos destinatários, exceto se relacionadas a uso legítimo da cooperativa;
10. Enviar mensagem por correio eletrônico pelo endereço de seu departamento ou usando o nome de usuário de outra pessoa ou endereço de correio eletrônico que não esteja autorizado a utilizar.
11. Divulgar informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação;
12. Apagar mensagens pertinentes de correio eletrônico quando qualquer uma das unidades da **CAPEBE** estiver sujeita a algum tipo de investigação
13. Produzir, transmitir ou divulgar mensagem que:
    a. Contenha ameaças eletrônicas, como: spam, phishing, mail bombing, malwares;
    b. Contenha arquivos com código executável (.exe, .cmd, .pif, .js, .hta, .src, cpl, .reg, .dll, .inf) ou qualquer outra extensão que represente um risco à segurança;
    c. Vise obter acesso não autorizado a outro computador, servidor ou rede;
    d. Vise interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
    e. Vise burlar qualquer sistema de segurança;
    f. Vise vigiar secretamente ou assediar outro usuário;
    g. Vise acessar informações confidenciais sem explícita autorização do proprietário;
    h. Tenha conteúdo considerado impróprio, obsceno ou ilegal;
    i. Seja de caráter calunioso, difamatório, degradante, infame, ofensivo, violento, ameaçador, pornográfico entre outros;
    j. Inclua material protegido por direitos autorais sem a permissão do detentor dos direitos.

REDES – INTERNET

A internet, atualmente considerada como essencial para a prestação da maioria dos serviços, representa um grande risco à instituição se não for utilizada dentro dos padrões éticos e profissionais estabelecidos pela cooperativa.

Desta forma, todas as informações que são acessadas, transmitidas, recebidas ou produzidas através da rede da **CAPEBE** são monitoradas e registradas pela cooperativa.

Também, os equipamentos, tecnologia e serviços fornecidos para o acesso à internet são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, site, correio eletrônico, domínio ou aplicação armazenados na rede/internet, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança da Informação.

A **CAPEBE**, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados **serão informados ao colaborador e ao respectivo gestor.**

O uso de qualquer recurso para atividades ilícitas poderá acarretar as ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A internet disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, excepcionalmente poderá ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos nas unidades com a sobrecarga da rede, o download de materiais ilícitos, a exposição da rede a riscos e o acesso a sites que vão contra os critérios estabelecidos nesta política.

Desta forma é preciso que sejam adotadas as seguintes medidas de segurança:

1. A Internet cabeada estará disponível apenas para máquinas e equipamentos de propriedade da **CAPEBE**, com a finalidade restrita à realização de atividade inerentes ao desempenho de tarefas laborais dos colaboradores nesta cooperativa.

2. A Internet sem fio deverá ser segregada, garantindo o isolamento da rede interna da cooperativa, com o objetivo de fornecer acesso a sistemas e dados internos apenas para os colaboradores desempenharem suas tarefas; poderá ter outras redes com acesso apenas à Internet para disponibilizar a visitantes e usuários que não precisam/podem ter acesso aos dados internos.
3. Os terceiros externos a Capebe deverão acessar o *wi-fi* disponibilizado aos visitantes. Este acesso será disponibilizado pelos colaboradores que tenham autorização para possuir a senha da rede externa.
4. Para além, os colaboradores que possuírem autorização da gestão direta do seu departamento também poderão utilizar o *wi-fi* da rede visitante pelo *smarthpone* pessoal. Por gestão direta compreendem-se os gerentes de departamento.
5. O RH ficará responsável por notificar formalmente o setor de infraestrutura sobre desligamentos de colaboradores, para que os acessos destes colaboradores sejam bloqueados e revogados;
6. É proibida a divulgação e/ou o compartilhamento indevido de informações internas, confidenciais e confidenciais restritas em listas de discussão, sites, redes sociais, fóruns, comunicadores instantâneos ou qualquer outra tecnologia correlata que use a internet com via, de forma deliberada ou inadvertidamente, sob a possibilidade de sofrer penalidades previstas nos procedimentos internos e/ou na forma da lei;
7. Os colaboradores com acesso à Internet só poderão fazer o download de programas necessários às suas atividades na **CAPEBE** e deverão providenciar a licença e o registro necessário desses programas, desde que autorizados pelo Coordenador do Setor respectivo e a diretoria;
8. O uso, a cópia ou a distribuição não autorizada de softwares que tenham direitos autorais, marca registrada ou patente são expressamente proibidos. Qualquer software não autorizado será excluído pelo setor de infraestrutura da **CAPEBE**;
9. Os colaboradores não poderão em hipótese alguma utilizar os recursos da **CAPEBE** para fazer o download ou distribuição de software ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional;

10. Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.
11. Documentos digitais de condutas consideradas ilícitas, como por exemplo, apologia ao tráfico de drogas e pedofilia, são expressamente proibidos e não devem ser acessados, expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso;
12. Os colaboradores não poderão usar os recursos da **CAPEBE** para deliberada ou inadvertidamente propagar qualquer tipo vírus, worms, cavalos de troia, spam, ou programas de controle remoto de outros computadores;
13. Não serão permitidos os acessos a softwares *peer-to-peer* (Kazaa, BitTorrent, µtorrent e afins);
14. Não serão permitidos os acessos a sites de compartilhamento de arquivos, tais como: mega, uploaded, bitshare, depositfiles, etc. Excepcionalmente o departamento de tecnologia da informação poderá fazer uso desses recursos mediante autorização do gerente do departamento.
15. Não serão permitidas tentativas de burlar os controles de acesso à rede, tais como utilização de proxies anônimos e estratégias de *bypass* de firewall;
16. Não serão permitidos o uso de aplicativos de reconhecimento de vulnerabilidades, análise de tráfego, ou qualquer outro que possa causar sobrecarga ou prejudicar o bom funcionamento e a segurança da rede interna, salvo os casos em que o objetivo for realizar auditorias de segurança, quando o setor de infraestrutura e desenvolvimento deverão estar devidamente cientes e concedido autorização para tal;
17. Os arquivos inerentes a **CAPEBE**, obrigatoriamente, deverão ser armazenados na pasta compartilhada de cada setor, localizada no servidor de arquivos e em sistemas utilizados pela cooperativa, para a garantia de backup destes documentos. É terminantemente proibido armazenar estes tipos de arquivos em equipamentos pessoais;
18. Não será permitida a alteração das configurações de rede e inicialização das máquinas bem como modificações que possam trazer algum problema futuro;

19. Haverá a geração de relatórios periódicos de sites e downloads acessados por usuários.

IDENTIFICAÇÃO

Os usuários devem ser identificados por meio de *login* e senha, isto porque este controle permite que haja a proteção da identidade do colaborador, de forma a possibilitar a manutenção da autenticidade e integridade das informações, além de prevenir que uma pessoa se faça passar por outra perante a **CAPEBE** e terceiros, o que constitui crime tipificado no Código Penal Brasileiro (Art. 307 – Falsa Identidade).

Assim, as normas aqui elencadas devem ser aplicadas a todos os colaboradores, gestores e diretores sem distinção, estabelecendo critérios e responsabilidades para o uso dos dispositivos de identificação.

Todos os dispositivos de identificação utilizados na **CAPEBE**, como o número de registro do colaborador, o crachá, as identificações de acesso aos sistemas, os certificados e assinaturas digitais e os dados biométricos têm de estar associados a uma pessoa física e atrelados inequivocamente aos seus documentos oficiais reconhecidos pela legislação brasileira.

O usuário, vinculado a tais dispositivos identificadores, será responsável pelo seu uso correto perante a instituição e a legislação (cível e criminal), não sendo permitido hipótese de utilização por outra pessoa, nem mesmo nos casos em que haja autorização do titular. Desta forma, em regra, todo e qualquer dispositivo de identificação pessoal não poderá ser compartilhado com outras pessoas em nenhuma hipótese.

No caso de haver *login* de uso compartilhado por mais de um colaborador, a responsabilidade perante a **CAPEBE** e a legislação (cível e criminal) **será dos usuários que dele se utilizarem,** somente sendo possível responsabilizar os gestores se for identificado conhecimento ou solicitação destes para o uso compartilhado.

Desta maneira, fica expressamente vedado o compartilhamento de login e senha para funções de administração de sistemas, sendo o departamento de Tecnologia da

Informação da **CAPEBE** responsável pela criação da identidade lógica dos colaboradores da cooperativa.

Os usuários de visitantes, estagiários, menores aprendizes, colaboradores temporários e regulares, além dos prestadores de serviços, pessoas físicas ou jurídicas devem ser identificadas de forma distinta.

Política de Senhas

Com o objetivo de orientar a criação de senhas seguras, estabelecem-se as seguintes regras:

1. A senha é de total responsabilidade do colaborador, sendo expressamente proibida sua divulgação ou empréstimo, devendo a mesma ser imediatamente alterada no caso de suspeita de sua divulgação;
2. A senha inicial será fornecida, prioritariamente ao próprio colaborador, pessoalmente, no dia da assinatura do contrato de trabalho. Não poderão ser fornecidas por comunicador instantâneo ou qualquer outra forma que não assegure a identidade do colaborador;
3. Ao realizar o primeiro acesso ao ambiente de rede local, o usuário deverá trocar imediatamente a sua senha conforme as orientações apresentadas.
4. As senhas não devem ser anotadas e deixadas próximo ao computador (debaixo do teclado, colada no monitor, etc.);
5. As senhas deverão seguir os seguintes pré-requisitos:
    a. Tamanho mínimo de oito caracteres;
    b. Existência de caracteres pertencentes a três dos seguintes grupos: letras maiúsculas, letras minúsculas e números;
    c. Não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word, Excel, etc.), compreensíveis por linguagem humana (não criptografados); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

6. O acesso do usuário deverá ser imediatamente **cancelado** quando houver desligamento do colaborador.
7. Também, o acesso do usuário deverá ser imediatamente **alterado** nas seguintes situações:
    a. Mudança de função de colaborador;
    b. Quando, por qualquer razão, cessar a necessidade de acesso do usuário ao sistema ou informação.
8. Para as alterações e os cancelamentos acima mencionados, o Departamento de Recursos Humanos da CAPEBE ficará responsável por informar prontamente ao setor de infraestrutura acerca dos desligamentos, mudança de função dos colaboradores e contratos cuja prestação de serviço tenha se encerrado.
9. O informe realizado pelo Departamento de Recursos Humanos citado no item anterior deverá ser feito no prazo máximo de 48hrs:
    a. Para mudança de funções, contado a partir da ciência da mudança de função;
    b. Para desligamento do colaborador, a partir da efetiva paralisação da prestação de serviço;
10. Os colaboradores que estiverem paralisados devido a mudança de função ou ao período de desligamento, também deverão ter os acessos suspensos, mesmo que ausente qualquer anotação na carteira de trabalho ou assinatura de rescisão contratual.
11. Os coordenadores e gerentes de setores que deixarem de informar ao departamento de Recursos Humanos sobre a mudança de função de e/ou desligamento de colaboradores serão responsabilizados por quaisquer danos advindos do acesso não autorizado destes colaboradores.
12. Em caso de esquecimento da senha, o colaborador deverá requisitar por telefone a troca ou comparecer à área técnica para cadastrar uma nova;
13. As requisições de troca de senha por telefone deverão ser realizadas mediante a comprovação do colaborador da sua identidade, através de solicitação do número de registro interno deste. Assim, o departamento de T.I responsável pela troca de senhas transmitirá ao colaborador senha padrão que contenha parte de

dado pessoal ou registro do colaborador, que deverá ser alterada após o primeiro acesso subsequente.

14. Após 6 (seis) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o setor de responsável pela troca e desbloqueio de senhas da CAPEBE pessoalmente ou por telefone, na solicitação por telefone deverá ser adotado o procedimento de confirmação de identidade através da solicitação de registro interno e elaboração de senha padrão para ser trocada após o primeiro acesso subsequente.
15. A periodicidade máxima para troca das senhas é 120 (cento e vinte) dias a partir da data de última alteração da senha, não podendo ser repetidas as 3 (três) últimas senhas, inclusive para os sistemas críticos e sensíveis para a instituição e os logins com privilégios administrativos. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo;

EQUIPAMENTOS E RECURSOS ELETRÔNICOS

A **CAPEBE** disponibiliza aos colaboradores dispositivos móveis e outros equipamentos eletrônicos para o melhor exercício laboral. Desta maneira, cabe aos colaboradores utilizá-los e manuseá-los corretamente, bem como cumprir todas as recomendações constantes nos procedimentos operacionais fornecidos pelas gerências responsáveis.

Caracteriza-se por dispositivo móvel qualquer equipamento eletrônico com atribuições de mobilidade, como: notebooks, *tablets* e *pendrives*, seja de propriedade da **CAPEBE** ou de propriedade particular, este último desde que possua prévia autorização para uso do gerente do departamento de tecnologia da informação da cooperativa.

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração, deslocamento ou modificação nos dispositivos móveis e equipamentos disponibilizados pela **CAPEBE**, sem o conhecimento prévio e o acompanhamento de um técnico do setor de infraestrutura, ou de quem este determinar.

As gerências que necessitarem fazer testes deverão solicitá-los previamente ao setor de infraestrutura, ficando responsáveis jurídica e tecnicamente pelas ações realizadas. Todas as atualizações e correções de segurança do sistema operacional ou

aplicativos somente poderão ser feitas após a devida validação no respectivo ambiente de homologação, e depois de sua disponibilização pelo fabricante ou fornecedor.

Os sistemas e computadores devem ter versões do software antivírus instaladas, ativadas e atualizadas permanentemente. O usuário, em caso de suspeita de vírus ou problemas na funcionalidade, deverá acionar o departamento técnico de infraestrutura mediante ligação telefônica ou e-mail.

A transferência e/ou a divulgação de qualquer software, programa ou instruções de computador para terceiros, por qualquer meio de transporte (físico ou lógico), somente poderá ser realizada com a devida identificação do solicitante, se verificada positivamente e estiver de acordo com a classificação de tal informação e com a real necessidade do destinatário.

Arquivos pessoais e/ou não pertinentes ao negócio da **CAPEBE** (fotos, músicas, vídeos, etc..) não deverão ser copiados/movidos para a rede interna, pois podem sobrecarregar o armazenamento nos servidores. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente por meio de comunicação prévia ao usuário.

Documentos imprescindíveis para as atividades dos colaboradores da instituição deverão ser salvos em drives de rede. Tais arquivos, se gravados apenas localmente nos computadores (por exemplo, no drive C:), não terão garantia de backup e poderão ser perdidos caso ocorra uma falha no computador, sendo, portanto, de responsabilidade do próprio usuário.

No uso dos computadores, equipamentos e recursos de informática, algumas regras devem ser atendidas:

1. Os colaboradores devem informar ao departamento técnico qualquer identificação de dispositivo estranho conectado ao seu computador.
2. Todos os modems internos ou externos devem ser removidos ou desativados para impedir a invasão/evasão de informações, programas, vírus. Em alguns casos especiais, conforme regra específica, será considerada a possibilidade de uso para planos de contingência mediante a autorização dos gestores das áreas e do setor de tecnologia da informação.

3. É expressamente proibido o consumo de alimentos, bebidas ou fumo na mesa de trabalho e próximo aos equipamentos.
4. O colaborador deverá manter a configuração do equipamento disponibilizado pelo **CAPEBE**, seguindo os devidos controles de segurança exigidos pela Política de Segurança da Informação e pelas normas específicas da instituição, assumindo a responsabilidade como custodiante de informações.
5. Deverão ser protegidos por senha (bloqueados), nos termos previstos pela Política de senha constante neste documento, todos os terminais de computador e impressoras quando não estiverem sendo utilizados.
6. Todos os recursos tecnológicos adquiridos pela **CAPEBE** devem ter imediatamente suas senhas padrões (default) alteradas.
7. Os equipamentos deverão manter preservados, de modo seguro, os registros de eventos, constando identificação dos colaboradores, datas e horários de acesso.

Dispositivos Móveis Pessoais

A **CAPEBE** veda o uso de dispositivos móveis pessoais dentro da instituição, exceto nas situações em que forem permitidos pelo coordenador/gestor do setor o uso de celulares e *smartphones*. Assim, somente será autorizado o uso de notebooks e demais dispositivos móveis quando houver flagrante necessidade ou urgência, mediante autorização do gerente de tecnologia da informação da cooperativa. Desta forma, nestes casos excepcionais os dispositivos móveis pessoais autorizados deverão seguir todas as regras do tópico “Estações de Trabalho” desta política, adicionalmente a:

1. Fica autorizado o uso de notebooks e dispositivos móveis para acesso à rede visitante da **CAPEBE** de prestadores de serviço, mediante autorização do coordenador imediato do setor responsável e autorização do gerente de tecnologia da informação da cooperativa;
2. O uso de notebooks e dispositivos móveis para fins de acesso à rede de Internet da **CAPEBE** para prestação de serviços, será realizado mediante a assinatura de termo de responsabilidade e ciência da política de segurança da informação pelo usuário que fará uso da internet.

3. É de responsabilidade do proprietário a instalação do Sistema Operacional que será utilizado, bem como dos aplicativos a serem utilizados no notebook, salvo exceções de aplicativos específicos autorizados pelo gerente de tecnologia da informação da Capebe;
4. É de responsabilidade do proprietário usar somente aplicativos legalizados em seu notebook;
5. Não podem ser executados nos notebooks aplicativos de característica maliciosa, que visam comprometer o funcionamento da rede, acesso a informações sem a devida permissão ou informações confidenciais;
6. É proibido o armazenamento de informações que não sejam de uso pessoal do proprietário do notebook. Todos os arquivos que pertençam a **CAPEBE** deverão ser excluídos do disco rígido do notebook e dos dispositivos de armazenamento móvel (ex: *pendrive*) assim que a prestação do serviço for finalizada;
7. Já nos computadores portáteis fornecidos pela **CAPEBE**, é proibido o armazenamento de informações confidenciais e confidenciais restritas no disco rígido do equipamento, devendo estas serem armazenadas nas pastas compartilhadas do servidor interno;
8. É proibida a inclusão de smartphones na rede corporativa da **CAPEBE**. Estes equipamentos deverão ter seu acesso restrito à rede de Internet;

Impressoras

O uso de impressoras na **CAPEBE** deve seguir algumas regras:

1. É proibida a impressão e xerox de documentos de cunho pessoal e/ou ilegal;
2. A configuração e manutenção das impressoras só podem ser realizadas pela equipe técnica da empresa responsável;
3. A instalação das impressoras deverá ser realizada por meio de solicitação ao setor de infraestrutura, sendo realizada por técnico do setor de Tecnologia da Informação;
4. O chefe de cada setor / unidade será o responsável pela impressora localizada na sala, inclusive para responder a questionamentos como impressões/xerox excessivas;

DATACENTER

As máquinas que constituem o servidor interno da cooperativa, onde são armazenados os sistemas e seus respectivos banco de dados, podem ser considerados importantes ativos para a cooperativa. Isto porque, estes permitem o essencial funcionamento dos sistemas tecnológicos da **CAPEBE** e o armazenamento dos seus ativos informacionais.

Estrutura física do datacenter

Desta forma, os servidores ficam localizados em área protegida dentro da Cooperativa, sendo o acesso físico devidamente controlado e monitorado, através de recurso biométrico. Assim, o acesso ao Datacenter somente se dará por sistema forte de autenticação, sendo devidamente registrado (usuário, data e hora) mediante o software de controle próprio.

O acesso biométrico ao Datacenter é controlado pelo coordenador da infraestrutura da cooperativa, sendo restrito aos colaboradores do setor de infraestrutura que precisam de acesso aos servidores e ao gerente de tecnologia da informação da **CAPEBE**.

Ademais, o acesso físico às dependências dos Servidores não poderá ocorrer com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, sendo autorizado somente quando houver expressa permissão do gestor do setor de Infraestrutura e mediante supervisão do responsável pelos servidores.

O acesso aos Servidores sem as devidas identificações só poderá ocorrer em emergências, quando a segurança física do local onde ficam armazenados for comprometida, como por incêndio, inundação, abalo da estrutura predial ou quando o sistema de autenticação não estiver funcionando.

Se houver necessidade de concessão de acesso definitivo ao ambiente físico do Datacenter para outros colaboradores, sem que haja a emergência, este acesso deverá ser diretamente solicitado ao coordenador do setor de infraestrutura por meio de memorando, para que haja liberação do colaborador.

O ambiente físico onde ficam armazenados os servidores deve ser mantido limpo e organizado, sendo vedada a entrada de qualquer tipo de alimento, bebida, produto fumígeno ou inflamável. Qualquer procedimento que gere lixo ou sujeira neste ambiente somente poderá ser realizado com a colaboração com o departamento de limpeza.

Aliado a isto, a entrada ou retirada de equipamentos do ambiente físico onde ficam armazenados os servidores somente se dará mediante solicitação do colaborador via Memorando ao coordenador do setor de infraestrutura, sendo autorizado por este.

Estrutura lógica do datacenter

Já no que concerne a alterações (leitura/edições) que possam ser efetuadas no ambiente lógico dos servidores, estas só poderão acontecer por meio dos analistas de Tecnologia da Informação da **CAPEBE**, mediante ciência do responsável pelo setor, obedecendo as atribuições da sua área de atuação.

Assim, os ativos de informações armazenados no servidor são protegidos de acessos indevidos e não autorizados, sendo que somente colaboradores credenciados do setor de desenvolvimento da tecnologia da informação poderão ter acessos. Desta maneira, os logs dos ativos de rede deverão ser monitorados constantemente afim de evitar acessos indevidos.

Prestadores de serviços de fornecedores de tecnologia também poderão obter acesso aos ambientes lógicos dos servidores quando necessário e mediante a assinatura de termo de declaração de responsabilidade e ciência das regras descritas neste documento e demais políticas atreladas a este, além da autorização do gerente de tecnologia da informação da Capebe.

Backup

O Backup pode ser tido como procedimento obrigatório para manutenção de um bom e seguro sistema da informação. É um procedimento essencial que garante cópias de segurança dos ativos da cooperativa, permitindo que a instituição esteja preparada para recuperar ou restaurar todos os seus dados de forma íntegra caso haja qualquer incidente de perda de dados.

Assim, deverá ser mantido em operação na cooperativa ferramentas que permitam o funcionamento do Datacenter mesmo diante do não funcionamento de algum Hack do servidor.

Visando isto, a Política de Backup da **CAPEBE** deverá seguir os seguintes procedimentos:

1. Deverá ser mantido em funcionamento nobreak dedicado a toda rede computacional da cooperativa, em caso de queda abrupta de energia. Aliado a este, gerador dedicado ao Datacenter que seja ativado automaticamente, para mitigar os riscos de queda de energia.
2. O banco de dados armazenado no Datacenter deverá ser replicado em outro local físico, para manutenção de redundância efetiva, por meio de canal fibrado.
3. Os servidores virtuais e estruturados deverão manter rotina periódica de backup.
4. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o software não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

AUDITORIA E FISCALIZAÇÃO DA POLÍTICA

A presente política deverá ter o seu cumprimento fiscalizado pelo departamento de tecnologia da informação da cooperativa, através da emissão periódica e mensal de relatórios que averiguem o uso da internet na cooperativa pelos colaboradores, tais como quantidades de download, acesso a sites, uso por hora de sites não atrelados ao exercício da função e entre outros.

Para mais, os presentes relatórios deverão analisar a quantidade de bloqueio de senhas, de concessão de acesso a rede visitante por prestadores de serviço, de tentativas de ataques aos sistemas internos da cooperativa e demais incidentes de segurança da informação.

Assim, após o prazo de 6 meses, os supracitados relatórios serão condessados em documento formal para avaliação da necessidade de alteração da Política de Segurança da Informação, conforme as necessidades da cooperativa. Essa avaliação

será feita nos 2 primeiros anos após a publicação desta política, após este prazo a avaliação de alteração da política poderá ser feita de ano em ano, a contar da data da última modificação.

DISPOSIÇÕES FINAIS

Esta política estabelece diretrizes e procedimentos para a implementação de uma cultura interna de segurança da informação e proteção de dados pessoais na **CAPEBE**. Desta forma, o descumprimento desta política será entendido como atuação contrária a ética e as boas práticas adotadas pela cooperativa, podendo ser puníveis com sanções