



POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Setembro de 2025

SUMÁRIO

1.	PRINCÍPIOS.....	4
2.	ABRANGÊNCIA	4
3.	NORMAS DE REFERÊNCIA.....	5
4.	DEFINIÇÕES.....	5
5.	OBJETIVOS	7
6.	DEVERES E RESPONSABILIDADES	7
7.	CLASSIFICAÇÃO DA INFORMAÇÃO	8
7.1.	Classificação da Informação	8
7.2.	Proteção e Sigilo das Informações	9
7.3.	Manutenção e Descarte de Informações	10
7.4.	Utilização de Conteúdo Protegido por Direitos Autorais	10
8.	Orientações de Segurança	11
8.1.	Privacidade	11
8.2.	Proteção de Dados Pessoais.....	12
8.3.	Proteção do Patrimônio Físico e Intangível.....	13
8.4.	Uso do E-mail	13
8.5.	Uso do Telefone Fixo.....	14
8.6.	Uso da Internet	14
8.7.	Uso das Impressoras.....	15
8.8.	Mesa Limpa	15
8.9.	Tela Limpa	15
8.10.	Senhas	15
8.11.	Trabalho Remoto (Home Office).....	16
9.	Gestão da Segurança Cibernética	17
9.1.	Autenticação e Controle de Acesso	17
9.1.1.	Serviços de Diretório	17
9.2.	Controle Contra Software Malicioso	18
9.3.	Atualizações.....	18
9.4.	Rastreabilidade	18

9.5.	Cópias de Segurança (Backup)	18
9.6.	Testes de Intrusão	19
9.7.	Varredura de Vulnerabilidades	19
10.	DESENVOLVIMENTO SEGURO	19
11.	Plano de Resposta a Incidentes de Segurança da Informação.....	20
12.	Gestão de Consequências	21
	Controle e Revisão.....	22

1. PRINCÍPIOS

A Vertrau reconhece que a informação é um dos ativos mais valiosos da organização, sendo essencial para a continuidade das operações, a confiança dos clientes e o cumprimento das exigências regulatórias. Assim, esta Política de Segurança da Informação e Segurança Cibernética foi elaborada para estabelecer diretrizes, controles, responsabilidades e comportamentos esperados que visam proteger as informações sob a custódia da empresa, incluindo dados internos, de clientes, parceiros e demais partes interessadas.

Os princípios fundamentais desta política são:

- **Confidencialidade:** Garantir que as informações sejam acessadas somente por pessoas autorizadas, no momento adequado e para finalidades legítimas.
- **Integridade:** Assegurar que a informação seja precisa, completa, válida e protegida contra alterações não autorizadas, acidentais ou maliciosas.
- **Disponibilidade:** Garantir que os dados e sistemas estejam acessíveis a usuários autorizados sempre que necessário, com resiliência contra falhas e incidentes.
- **Autenticidade:** Assegurar a identificação e verificação da identidade dos usuários e sistemas envolvidos no processamento de dados.
- **Responsabilidade:** Definir e comunicar as responsabilidades dos colaboradores, parceiros e prestadores de serviços em relação ao tratamento e à proteção da informação.
- **Rastreabilidade:** Implementar mecanismos que permitam auditar os acessos, transações e alterações feitas sobre os dados e sistemas.

Esta política orienta todas as ações relacionadas ao ciclo de vida da informação, desde sua criação, armazenamento e uso até seu descarte seguro, promovendo uma cultura organizacional voltada à segurança da informação.

2. ABRANGÊNCIA

A presente política é obrigatória para todas as pessoas e entidades que, de forma direta ou indireta, tenham acesso a ativos de informação da Vertrau. Isso inclui, mas não se limita a:

- Colaboradores (incluindo estagiários, aprendizes e terceirizados);
- Sócios, administradores e membros da diretoria;
- Fornecedores de tecnologia e serviços que tenham acesso a sistemas, dados ou infraestrutura da Vertrau;
- Parceiros de negócios que realizem integração de dados ou compartilhem sistemas com a Vertrau;
- Consultores, auditores e prestadores de serviços especializados;
- Demais partes que, por qualquer razão, atuem com informações de propriedade da Vertrau ou sob sua custódia.

Todos os envolvidos devem cumprir esta política, independentemente da natureza do vínculo, regime de contratação ou localidade geográfica. A aceitação e a adesão às normas aqui estabelecidas são condições indispensáveis para o acesso e uso de sistemas, plataformas, dados ou documentos institucionais.

3. NORMAS DE REFERÊNCIA

A Vertrau adota como base legal e normativa os seguintes regulamentos e diretrizes de segurança da informação e proteção de dados:

- **Resolução BCB nº 85/2021:** Estabelece diretrizes para a estrutura de gerenciamento de segurança cibernética nas instituições reguladas pelo Banco Central do Brasil.
- **Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD):** Define o tratamento adequado e legal de dados pessoais por agentes públicos e privados.
- **Guia de Cibersegurança da ANBIMA:** Conjunto de boas práticas recomendadas para instituições participantes do mercado financeiro, especialmente gestoras, administradoras e distribuidoras.

4. DEFINIÇÕES

Para os fins desta Política, são adotadas as seguintes definições:

- **Ativos de Informação:** Qualquer dado, sistema, aplicação, banco de dados, meio físico ou digital, dispositivo ou estrutura que armazene ou processe informação relevante.
- **Ativos Físicos:** Computadores, servidores, dispositivos móveis, roteadores, cabos de rede, impressoras, mídias removíveis, entre outros.
- **Ativos de Software:** Sistemas operacionais, aplicações desenvolvidas ou adquiridas, APIs, bibliotecas, licenças e ferramentas de monitoramento.
- **Confidencialidade:** Garantia de que a informação seja acessível somente por pessoas autorizadas.
- **Integridade:** Preservação da exatidão e completeza da informação durante todo o seu ciclo de vida.
- **Disponibilidade:** Acesso garantido à informação e aos sistemas sempre que necessário por usuários legitimados.
- **Autenticidade:** Garantia de que um dado, transação ou mensagem tenha origem legítima e reconhecível.
- **Backup:** Cópia de segurança de dados e sistemas realizada com objetivo de recuperação em caso de falhas, perdas ou ataques.
- **Criptografia:** Técnica de codificação de informações para torná-las ilegíveis a terceiros não autorizados.
- **Incidente de Segurança:** Qualquer evento que coloque em risco a confidencialidade, integridade ou disponibilidade de um ativo de informação.
- **Malware:** Programa malicioso capaz de causar danos ou comprometer dispositivos e redes.
- **Spam:** Mensagens eletrônicas enviadas em massa, geralmente sem consentimento do destinatário, com intuito comercial ou fraudulento.
- **Trojan (Cavalo de Troia):** Tipo de malware que se disfarça de software legítimo para obter acesso indevido ao sistema da vítima.
- **Rastreabilidade:** Capacidade de reconstruir a sequência de ações realizadas sobre um sistema, arquivo ou dado.

5. OBJETIVOS

Os objetivos da Política de Segurança da Informação e Cibernética da Vertrau são os seguintes:

- **Garantir conformidade regulatória:** Assegurar que a empresa atue em conformidade com legislações e normativas aplicáveis, como LGPD, Resolução BCB nº 85/2021 e demais regulamentos de órgãos fiscalizadores.
- **Proteger dados sensíveis:** Implementar mecanismos de proteção eficazes para prevenir vazamentos, acessos não autorizados e incidentes que possam comprometer informações pessoais, operacionais, financeiras ou estratégicas.
- **Reduzir riscos operacionais:** Antecipar, identificar e mitigar ameaças que possam afetar a continuidade do negócio, a reputação institucional ou a integridade dos sistemas e dados.
- **Preservar a imagem institucional:** Adotar práticas que reforcem a confiança de clientes, parceiros e reguladores, demonstrando compromisso com a segurança da informação.
- **Promover cultura organizacional segura:** Disseminar conhecimento, boas práticas e diretrizes entre os colaboradores e parceiros, para que todos compreendam e atuem de forma responsável frente ao tratamento das informações.
- **Implementar controles técnicos e administrativos:** Estabelecer, monitorar e revisar controles que garantam o correto gerenciamento dos riscos de segurança da informação e cibernética.

6. DEVERES E RESPONSABILIDADES

Os colaboradores da Vertrau são peças-chave para o sucesso da política de segurança da informação. Portanto, espera-se de cada colaborador o comprometimento com os seguintes deveres:

- a) Preservar a integridade e guardar sigilo das informações de que fazem uso, bem como zelar e proteger os respectivos recursos de processamento de informações;

- b) Cumprir a presente Política, sob pena de incorrer nas sanções disciplinares e legais cabíveis;
- c) Utilizar os sistemas de informações e os recursos relacionados somente para atividades necessárias cumprimento das atividades de negócios;
- d) Cumprir as regras específicas de proteção estabelecidas aos Ativos de informação;
- e) Manter o caráter sigiloso de senhas de acesso aos recursos e sistemas, sem compartilhar acessos ou permitir usos por outras pessoas (“caronas”);
- f) Não compartilhar, sob qualquer forma, informações confidenciais com outros que não tenham a devida autorização de acesso;
- g) Responder por todo e qualquer acesso aos recursos da Vertrau, bem como pelos efeitos decorrentes de acesso efetivado através de seu código de identificação, ou outro atributo para esse fim utilizado;
- h) Solicitar acesso a informações restritas somente quando houver real necessidade de acessar o recurso;
- i) Respeitar a proibição de não usar, inspecionar, copiar ou armazenar programas de computador ou qualquer outro material, sob pena de violação da legislação de propriedade intelectual pertinente;

O não cumprimento dessas obrigações poderá gerar responsabilizações de natureza disciplinar, cível ou até criminal, conforme a gravidade do ocorrido e os danos decorrentes do incidente.

7. CLASSIFICAÇÃO DA INFORMAÇÃO

A gestão da informação na Vertrau tem como objetivo assegurar que os dados e ativos informacionais sejam devidamente protegidos, classificados, armazenados, acessados e compartilhados conforme critérios de segurança, confidencialidade e integridade. Todos os colaboradores, parceiros e prestadores de serviços devem seguir as orientações abaixo com rigor.

7.1. Classificação da Informação

Todas as informações manipuladas na Vertrau, independentemente de sua origem ou formato, devem ser classificadas de acordo com o seu grau de sensibilidade. A classificação adequada assegura o tratamento proporcional aos riscos e às exigências legais e contratuais.

As categorias de classificação da Vertrau são:

Nível de Classificação	Definição	Exemplos
Confidencial	Informações que, se acessadas ou divulgadas indevidamente, podem gerar impactos severos à Vertrau, seus clientes ou parceiros. Acesso limitado e altamente restrito.	Documentos estratégicos, planos de negócio, dados financeiros sensíveis, informações pessoais sensíveis, resultados de auditoria, credenciais administrativas, segredos industriais.
Restrita	Informações importantes para os negócios, acessíveis apenas a áreas específicas ou grupos autorizados.	Contratos com clientes, documentos internos de projetos, dados cadastrais de clientes e fornecedores, material de due diligence.
Uso Interno	Informações voltadas para uso exclusivo dos colaboradores, mas cujo vazamento não causa danos significativos.	Políticas internas, organogramas, atas de reunião internas, políticas e manuais não públicos, templates de documentos.
Pública	Informações que podem ser livremente divulgadas sem risco à Vertrau.	Conteúdo institucional, apresentações públicas, campanhas de marketing, materiais publicados no site.

Todos os documentos, sistemas e fluxos devem conter, sempre que possível, identificação explícita de sua classificação. A ausência de marcação **não** isenta o conteúdo de tratamento seguro.

7.2. Proteção e Sigilo das Informações

A Vertrau estabelece os seguintes princípios de conduta em relação à proteção de dados e informações:

Confidencialidade contínua: as obrigações de sigilo permanecem mesmo após o desligamento do colaborador ou término de contrato com terceiros.

Compartilhamento responsável: informações só podem ser compartilhadas com pessoas autorizadas e mediante necessidade clara de negócio.

Armazenamento seguro: documentos e dados sensíveis devem estar em repositórios com controle de acesso, criptografia (quando aplicável), e preferencialmente em ambiente em nuvem homologado pela Vertrau.

Comunicação verbal: conversas sobre temas confidenciais não devem ocorrer em ambientes públicos (corredores, restaurantes, elevadores, etc.).

Transporte e cópia: não é permitido copiar documentos confidenciais para dispositivos pessoais, enviar para e-mails externos ou armazenar sem proteção adequada.

7.3. Manutenção e Descarte de Informações

A Vertrau adota práticas de governança da informação com foco em eliminação segura e retenção adequada:

Descarte físico: documentos confidenciais devem ser destruídos com fragmentadoras ou por empresas especializadas.

Descarte digital: arquivos devem ser excluídos permanentemente dos sistemas e lixeiras digitais. Dispositivos descartados ou reutilizados devem passar por formatação segura realizada pela equipe de TI.

Limpeza periódica: arquivos antigos, duplicados ou desnecessários devem ser eliminados periodicamente, em especial os que contêm dados pessoais ou estratégicos.

Migração e backup: arquivos não devem permanecer apenas em discos locais. Todo material relevante deve estar salvo nos diretórios institucionais da Vertrau, passíveis de backup regular.

7.4. Utilização de Conteúdo Protegido por Direitos Autorais

A Vertrau reconhece a importância da proteção à propriedade intelectual e adota diretrizes rigorosas para evitar o uso indevido de materiais protegidos por direitos autorais em suas operações. Todos os colaboradores devem observar as seguintes orientações:

- a) Não é permitido copiar, reproduzir, distribuir ou utilizar softwares, imagens, músicas, vídeos, textos, marcas, logotipos ou qualquer outro conteúdo

- protegido por direitos autorais, sem a devida autorização do titular ou licenciamento adequado;
- b) A utilização de imagens, músicas ou vídeos em apresentações, materiais de comunicação interna ou externa e em sistemas da Vertrau só é permitida quando:
 - i) forem de domínio público;
 - ii) estiverem sob licenças permissivas (como Creative Commons, quando aplicável);
 - iii) houver comprovação de compra ou cessão de uso por parte da Vertrau.
 - c) É terminantemente proibido o uso de imagens ou marcas registradas de terceiros que possam causar associação indevida com a Vertrau, ou que não tenham sido autorizadas formalmente;
 - d) O download de softwares, arquivos ou conteúdo de fontes não autorizadas ou não verificadas é vedado. Qualquer necessidade de software ou recurso externo deve ser encaminhada previamente para validação da equipe de Segurança da Informação e Tecnologia;
 - e) Em caso de dúvidas quanto ao uso legal de determinado conteúdo, o colaborador deve consultar a área Jurídica ou de Segurança da Informação antes de proceder com sua utilização;
 - f) A violação dos direitos autorais por parte de qualquer colaborador ou prestador poderá acarretar penalidades contratuais, administrativas, civis e criminais, além de danos à imagem institucional da Vertrau.

8. Orientações de Segurança

Este capítulo estabelece diretrizes práticas para o uso seguro e responsável dos ativos físicos, digitais e informacionais da Vertrau, garantindo conformidade com normas internas, legais e regulatórias.

8.1. Privacidade

A Vertrau se reserva o direito de acessar e monitorar informações armazenadas ou processadas em seus equipamentos, sistemas, redes e ambientes em nuvem, inclusive aquelas localizadas fisicamente em instalações da empresa, como mesas, gavetas e armários. Esse acesso pode ocorrer mesmo sem o consentimento prévio do colaborador, desde que haja justificativa técnica, operacional ou regulatória.

As comunicações realizadas por meios corporativos – como e-mails, ligações telefônicas e mensagens internas – também podem ser monitoradas e armazenadas, com o objetivo de garantir a segurança da informação e o cumprimento das políticas internas. A escuta de chamadas e leitura de mensagens depende de autorização expressa da equipe de Segurança da Informação.

A Vertrau compromete-se a tratar com sigilo quaisquer dados acessados no processo de monitoramento, inclusive informações de natureza pessoal.

Qualquer incidente ou suspeita de violação de privacidade deve ser imediatamente reportado pelos canais oficiais e registrado no sistema de compliance da organização. Os colaboradores devem também observar as diretrizes constantes na Política de Privacidade e Proteção de Dados Pessoais da Vertrau.

8.2. Proteção de Dados Pessoais

A Vertrau coleta e trata dados pessoais de usuários, clientes e parceiros de acordo com a Lei Geral de Proteção de Dados (LGPD), respeitando os princípios da legalidade, necessidade, transparência e segurança.

Durante a navegação em seus sistemas ou websites, mesmo sem cadastro, podem ser coletadas informações como endereço IP, tipo e versão do navegador, sistema operacional, geolocalização, modelo do dispositivo, comportamento de navegação e dados técnicos da conexão.

Nos cadastros realizados pelos usuários, poderão ser fornecidos dados pessoais como nome completo, documentos de identidade, endereço, e-mail, telefone, dados bancários, informações profissionais e dados relacionados à situação financeira e vínculo com pessoas politicamente expostas.

A Vertrau poderá complementar essas informações por meio de fontes externas, como bureaus de crédito, com o objetivo de validar identidade, detectar fraudes e cumprir obrigações legais ou regulatórias.

A titularidade do cadastro é pessoal e intransferível, e apenas o próprio titular pode atualizar seus dados. Caso sejam identificadas inconsistências ou indícios de risco, a Vertrau poderá solicitar documentação adicional ou, se necessário, suspender ou encerrar o relacionamento com o titular.

Erros ou omissões no fornecimento de dados são de responsabilidade exclusiva do titular, que deve manter suas informações sempre atualizadas.

8.3. Proteção do Patrimônio Físico e Intangível

O patrimônio da Vertrau compreende seus imóveis, equipamentos, sistemas, dados, informações estratégicas, produtos, tecnologias, marcas, planos de negócio, pesquisas e demais ativos tangíveis e intangíveis. Esses bens devem ser preservados e utilizados exclusivamente para fins profissionais e no interesse da empresa.

É vedado utilizar os recursos da Vertrau para fins pessoais, salvo em casos autorizados previamente pelo gestor responsável e desde que não:

- a) Prejudiquem ou concorram com as atividades da Vertrau;
- b) Envolvam o fornecimento de informações a terceiros;
- c) Tenham finalidade comercial alheia à empresa;
- d) Gerem custos adicionais à Vertrau.

O uso indevido dos ativos da empresa, bem como o seu compartilhamento externo sem autorização, é passível de medidas disciplinares e legais.

8.4. Uso do E-mail

O e-mail corporativo da Vertrau é uma ferramenta institucional voltada à comunicação profissional, devendo ser utilizado com responsabilidade, civilidade e foco na produtividade.

As diretrizes incluem:

- e) O colaborador é o único responsável por todas as mensagens enviadas por sua conta;
- f) O uso é preferencialmente profissional, sendo permitido uso pessoal com bom senso, desde que não conflite com os interesses da Vertrau nem viole leis ou políticas internas;
- g) É proibido abrir anexos de origem desconhecida ou executar programas suspeitos;
- h) É vedado o envio de spam, mensagens em massa, conteúdos ilegais, ofensivos ou que infrinjam direitos de terceiros;
- i) O envio de materiais que contenham vírus, malwares ou programas prejudiciais é estritamente proibido;
- j) Mensagens confidenciais não devem ser impressas em impressoras compartilhadas sem o devido cuidado;
- k) O e-mail deve permanecer ativo durante o expediente, e o usuário deve bloquear sua estação de trabalho ao se ausentar;

- l) Administradores de e-mail não têm permissão para acessar mensagens de outros usuários, salvo em casos autorizados pela equipe de Segurança da Informação ou por determinação legal;
- m) É proibido enviar arquivos que comprometam a rede da Vertrau ou que infrinjam leis de direitos autorais.

8.5. Uso do Telefone Fixo

O telefone fixo corporativo da Vertrau deve ser utilizado prioritariamente para fins profissionais. O uso pessoal é permitido com bom senso, desde que não conflite com as atividades da empresa ou viole normas legais e internas.

- a) Todas as ligações podem ser gravadas e monitoradas;
- b) Em situações excepcionais, ligações confidenciais feitas fora da Vertrau devem ser realizadas com cautela, evitando exposição a terceiros;
- c) Não se deve deixar mensagens sensíveis em secretárias eletrônicas;
- d) Teleconferências e videoconferências devem ser iniciadas apenas após a confirmação da identidade e autorização de todos os participantes.

8.6. Uso da Internet

O acesso à internet em dispositivos da Vertrau ou em rede corporativa deve priorizar atividades profissionais e seguras.

- a) É proibido acessar sites com conteúdo impróprio ou distribuir materiais inadequados ao ambiente de trabalho;
- b) O uso de serviços de mensagens (como WhatsApp ou similares) e redes sociais (como Facebook, LinkedIn, Instagram, X) é permitido para fins profissionais, ou pessoais com moderação, desde que não conflite com os interesses da Vertrau nem viole regras internas;
- c) Toda comunicação realizada em dispositivos da Vertrau poderá ser monitorada, sendo proibido compartilhar assuntos institucionais sem autorização da equipe de Segurança da Informação;
- d) É vetado o acesso a e-mails pessoais em dispositivos da Vertrau, salvo exceções autorizadas;
- e) É proibido o uso de redes peer-to-peer (P2P) e o download de arquivos não autorizados, como músicas e vídeos;
- f) O uso de streaming de áudio é permitido com moderação. Streaming de vídeo só será autorizado com consentimento prévio da equipe de Segurança da Informação.

8.7. Uso das Impressoras

O uso das impressoras na Vertrau deve ser consciente, seguro e voltado para fins profissionais.

- a) Impressões contendo informações confidenciais devem ser retiradas imediatamente após o envio;
- b) Só devem ser impressos documentos cuja versão física seja realmente necessária, evitando desperdícios;
- c) Impressões pessoais são permitidas com moderação, desde que não conflitem com os interesses da Vertrau nem violem normas internas ou legais.

8.8. Mesa Limpa

A política de mesa limpa tem como objetivo proteger informações e dispositivos físicos contra acessos indevidos.

- a) Nenhum documento confidencial, mídia removível ou equipamento da Vertrau deve ficar desprotegido em estações de trabalho desocupadas;
- b) Ao final do expediente, notebooks devem ser guardados com segurança ou levados pelo responsável, conforme orientação do gestor da área.

8.9. Tela Limpa

Para garantir a proteção das informações, todos os dispositivos devem estar bloqueados quando não estiverem em uso.

- a) É obrigatório o uso de proteção de tela com senha automática, com tempo máximo de 5 minutos de inatividade;
- b) A senha deve ser pessoal, intransferível e nunca deixada anotada em local acessível.

8.10. Senhas

A Vertrau adota uma política rigorosa para criação e manutenção de senhas de acesso.

- a) As senhas devem ser trocadas obrigatoriamente a cada 60 dias;
- b) Devem conter no mínimo 8 caracteres, com pelo menos um número e um caractere especial;

- c) As senhas não podem ser óbvias, como senhas sequenciais (ex.: sequências numéricas ou alfabéticas) ou derivadas de dados pessoais (ex.: nome ou data de nascimento do usuário);
- d) A senha representa a assinatura digital do colaborador, sendo sua guarda e sigilo de responsabilidade individual;
- e) O acesso concedido por senha será limitado às funções necessárias de cada colaborador e poderá ser revogado a qualquer momento, conforme necessidade de segurança.

8.11. Trabalho Remoto (Home Office)

A Vertrau adota o modelo de trabalho híbrido ou remoto conforme necessidade operacional, mantendo os padrões de segurança aplicáveis aos ambientes corporativos.

As seguintes diretrizes devem ser observadas pelos colaboradores em regime de home office:

- a) O colaborador deve utilizar equipamentos corporativos sempre que possível, com sistemas atualizados e protegidos por antivírus oficial;
- b) O acesso a sistemas internos deve ocorrer exclusivamente por conexões seguras, preferencialmente via VPN corporativa;
- c) É proibido o uso de redes Wi-Fi públicas ou não protegidas por senha;
- d) Dispositivos pessoais só poderão ser utilizados mediante autorização prévia da equipe de Segurança da Informação;
- e) Documentos físicos e digitais devem ser mantidos sob guarda segura, evitando visualização por pessoas não autorizadas;
- f) É vedado o armazenamento local de arquivos confidenciais em dispositivos pessoais;
- g) O ambiente doméstico deve seguir as práticas de mesa limpa e tela limpa, mesmo fora das dependências da Vertrau;
- h) Em caso de perda, roubo ou suspeita de comprometimento do equipamento, o colaborador deve comunicar imediatamente a equipe de Segurança da Informação;
- i) O uso de mídias removíveis (pendrives, HDs externos, etc.) deve ser evitado e, quando necessário, deve ocorrer apenas com mídias criptografadas e aprovadas.

9. Gestão da Segurança Cibernética

9.1. Autenticação e Controle de Acesso

A Vertrau adota práticas rigorosas de controle de acesso com o objetivo de proteger seus ambientes e sistemas contra acessos indevidos, garantindo a confidencialidade, integridade e disponibilidade das informações.

As diretrizes incluem:

- a) Atribuição de acessos com base em matriz de segregação de funções, considerando equipes, perfis e níveis de autorização;
- b) Aplicação do princípio do menor privilégio, com concessão apenas ao necessário para o exercício da função;
- c) Processos formalizados para concessão, alteração e revogação de acessos, sempre com aprovação do gestor da área;
- d) Os acessos são limitados aos ativos sob responsabilidade da equipe do gestor, e o gestor é responsável por informar a necessidade de acesso em novas admissões;
- e) Acessos transversais (entre áreas diferentes) são autorizados pelos dois gestores envolvidos: o da equipe e o do sistema-alvo;
- f) A Vertrau realiza revisão anual de acessos, coordenada pela área de Segurança da Informação;
- g) Regras de acesso também se aplicam a ambientes de contingência e continuidade de negócios, preservando os mesmos critérios de segurança.

9.1.1. Serviços de Diretório

A Vertrau utiliza um serviço de diretório em nuvem baseado no Azure Active Directory (AD), fornecido pela Microsoft, como principal mecanismo de autenticação e gestão de identidade.

- a) Todos os colaboradores utilizam suas credenciais corporativas do Microsoft 365 para acessar os sistemas internos, aplicações em nuvem, serviços de e-mail, recursos de produtividade e demais soluções integradas ao ambiente corporativo.
- b) Esse diretório permite o compartilhamento e controle centralizado de informações de usuários, grupos, permissões, senhas e políticas de acesso, promovendo segurança e padronização.
- c) Sempre que possível, os sistemas adquiridos ou desenvolvidos pela Vertrau são integrados ao Azure AD, garantindo uma autenticação única (Single Sign-On) e uma experiência segura e simplificada para os usuários.

9.2. Controle Contra Software Malicioso

A Vertrau adota medidas proativas para proteger seus ativos contra softwares maliciosos (malwares), como vírus, trojans e ransomwares.

- a) Todos os dispositivos corporativos devem possuir antivírus atualizado automaticamente;
- b) É proibido acessar ou encaminhar alertas suspeitos que não sejam gerados pelo antivírus oficial;
- c) Em caso de dúvida sobre alertas ou possíveis ameaças, o colaborador deve imediatamente acionar a equipe de Segurança da Informação para esclarecimento e suporte.

9.3. Atualizações

A atualização constante de sistemas é essencial para manter a segurança da infraestrutura da Vertrau.

- a) Os sistemas operacionais, antivírus e demais softwares devem estar sempre com as atualizações automáticas habilitadas;
- b) Exceções serão permitidas apenas em casos justificados, como testes em ambientes controlados ou incompatibilidade com sistemas legados, sempre sob supervisão técnica.

9.4. Rastreabilidade

Todas as soluções da Vertrau — adquiridas ou desenvolvidas internamente — devem possuir mecanismos de log e trilhas de auditoria.

- a) Os logs devem registrar eventos críticos, acessos, falhas e interações com o sistema, possibilitando análises técnicas e auditorias;
- b) Trilhas automatizadas devem ser implantadas em todos os sistemas para garantir a reconstrução de eventos, rastreabilidade de ações e responsabilização de usuários em casos de anomalias ou incidentes.

9.5. Cópias de Segurança (Backup)

A Vertrau considera os processos de backup essenciais para garantir a continuidade operacional.

- a) Todos os arquivos relacionados ao negócio devem ser armazenados em pastas centralizadas, localizadas em servidores ou serviços de nuvem gerenciados pela empresa;

- b) Cada colaborador possui uma pasta profissional individual e uma estrutura compartilhada com sua equipe;
- c) Arquivos armazenados localmente nos computadores não são cobertos pelos processos de backup e são de inteira responsabilidade do usuário;
- d) O armazenamento em nuvem garante maior segurança e recuperação eficiente em caso de incidentes.

9.6. Testes de Intrusão

A Vertrau realiza testes de intrusão (pentests) internos e externos de forma programada, visando identificar vulnerabilidades em suas redes e aplicações. Esses testes são fundamentais para fortalecer a segurança do ambiente tecnológico e devem ser executados no mínimo uma vez ao ano. A realização de testes sem autorização prévia é proibida e sujeita a medidas disciplinares.

- a) Testes devem abranger redes, aplicações internas e aplicações desenvolvidas por terceiros;
- b) Apenas empresas formalmente contratadas podem realizar pentests;
- c) Testes não autorizados são considerados violações graves e serão investigados;
- d) O objetivo é detectar, corrigir e prevenir vulnerabilidades críticas antes que possam ser exploradas.

9.7. Varredura de Vulnerabilidades

A Vertrau realiza varreduras de vulnerabilidades para identificar falhas de segurança de forma contínua e preventiva, tanto nas redes internas quanto externas.

- a) Varreduras devem ser realizadas periodicamente e após mudanças relevantes na infraestrutura;
- b) As vulnerabilidades identificadas devem ser registradas, analisadas e priorizadas conforme seu nível de criticidade;
- c) A tratativa das vulnerabilidades deve seguir planos de correção adequados ao risco identificado;
- d) As ações corretivas devem ser monitoradas até a completa resolução do problema.

10. DESENVOLVIMENTO SEGURO

A Vertrau adota práticas robustas de desenvolvimento seguro, assegurando que os princípios de segurança cibernética sejam incorporados desde as fases iniciais do

ciclo de vida dos sistemas. A empresa mantém diretrizes claras para a segregação de ambientes, controle de acessos e validação de qualidade de código, garantindo a integridade e a confiabilidade das soluções desenvolvidas internamente ou por terceiros.

- e) Os ambientes de produção, desenvolvimento, testes/homologação e pré-produção são segregados fisicamente, logicamente e administrativamente;
- f) O acesso aos ambientes de produção é restrito e concedido apenas mediante autorização expressa da equipe de Segurança da Informação;
- g) As áreas de segurança e negócios atuam em conjunto para:
 - i) Estabelecer requisitos específicos de segurança durante o desenvolvimento e manutenção de sistemas;
 - ii) Minimizar riscos como fraudes, vazamento de dados e acessos indevidos;
 - iii) Acompanhar projetos segundo metodologias de desenvolvimento adotadas pela Vertrau;
- h) Todos os sistemas devem permitir registro de logs e trilhas de auditoria, assegurando a rastreabilidade de ações e alterações;
- i) Alterações em sistemas em produção — incluindo novas versões e correções de bugs — devem ser revisadas e aprovadas por um usuário supervisor nomeado pela Diretoria de Tecnologia da Informação;
- j) A Vertrau realiza avaliações técnicas e métricas da segurança do código fonte, tanto em sistemas internos quanto em sistemas desenvolvidos por fornecedores externos, com foco em qualidade e mitigação de riscos.

11. Plano de Resposta a Incidentes de Segurança da Informação

As respostas aos incidentes de Segurança da Informação visam assegurar o restabelecimento do nível normal do ambiente tecnológico, após o acontecimento de um sinistro, fornecendo direcionamento para a devida utilização dos recursos e procedimentos fundamentais, garantindo efetividade.

O plano abrange incidentes originados tanto em sistemas de desenvolvimento interno, como em sistemas de empresas prestadoras de serviços.

O plano contempla as seguintes fases:

- a) **Planejamento:** identificação prévia de cenários de risco, definição de ações de mitigação, responsáveis, prazos e registros para facilitar a atuação em situações reais;
- b) **Identificação:** detecção e registro formal dos incidentes que afetam ou possam afetar a segurança da informação;

- c) **Resposta:** aplicação imediata de medidas técnicas e operacionais para conter, mitigar e tratar o incidente detectado;
- d) **Vistoria:** auditorias, análises de vulnerabilidades e investigações posteriores para entender a causa raiz e evitar recorrências;
- e) **Compartilhamento:** comunicação de incidentes relevantes às autoridades competentes, como o Banco Central do Brasil (BACEN), a Autoridade Nacional de Proteção de Dados (ANPD), e, quando aplicável, instituições financeiras ou prestadores de serviço parceiros.

12. Gestão de Consequências

A Vertrau adota o princípio de que o desconhecimento das normas de segurança não isenta o colaborador de responsabilidade. Todos os envolvidos devem conhecer e cumprir as disposições desta política.

- a) Violações às diretrizes estabelecidas podem resultar em medidas administrativas, disciplinares, civis ou criminais, conforme a gravidade da infração;
- b) Em caso de dúvidas sobre o conteúdo da política ou suas aplicações, o colaborador deve procurar a Diretoria de Riscos ou a Equipe de Segurança da Informação;
- c) A Vertrau incentiva o esclarecimento prévio e a comunicação transparente como forma de prevenção de incidentes.

Controle e Revisão

Registro de Alterações			
Área responsável pela Norma		Riscos e Segurança da Informação	
Versão	Data	Responsável	Alterações
V1	26/12/2024	Dionathan Henschel	Elaboração do documento
V2	07/08/2025	Dionathan Henschel	Ajustes no desenvolvimento seguro
V3	10/09/2025	Dionathan Henschel	Inclusão do item 8.11 – Home office
Classificação da Informação		Uso Interno	