PONTIFÍCIA UNIVERSIDADE CATÓLICA DE MINAS GERAIS

INSTITUTO DE CIÊNCIAS EXATAS E INFORMÁTICA

Bacharelado em Sistemas de Informação

André Fabiano de Andrade Lima

Beatriz Fontainha de Castro

Luiz Henrique Santos de Andrade

Matheus Carlos Fraga dos Santos

Ramir Aguiar Ribeiro Junior

Sibelle Mendes Diniz

Projeto da Infraestrutura de Rede:

Política de Segurança da Informação – Telemarketing

Teleconnect

Belo Horizonte

2025

Objetivo

O objetivo desta Política de Segurança da Informação é estabelecer as diretrizes e controles necessários para proteger as informações da organização, garantindo que os dados sejam tratados de forma segura e responsável por todos os colaboradores, prestadores de serviço e parceiros.

As diretrizes que serão apresentadas são baseadas nos três pilares fundamentais da Segurança da Informação:

- Confidencialidade: assegurar que a informação seja acessada apenas por pessoas autorizadas.
- Integridade: garantir que a informação seja mantida exata, completa e protegida contra alterações não autorizadas.
- Disponibilidade: garantir que as informações e recursos estejam disponíveis aos usuários autorizados sempre que necessário.

Além disso, essa Política visa assegurar a conformidade com as legislações vigentes, incluindo a **Lei Geral de Proteção de Dados Pessoais (LGPD)**.

Abrangência

Esta política se aplica a:

- Todos os colaboradores, contratados e prestadores de serviço, da matriz e filiais;
- Todos os sistemas de informação, hardware, software, redes e infraestrutura tecnológica.
- Todas a informações armazenadas, processadas ou transmitidas pela empresa, independentemente do meio.

Glossário

Acesso Restrito: Permissão para visualizar ou usar informações e sistemas apenas por pessoas autorizadas, com base na necessidade para o trabalho.

Autenticação Multifator (MFA): Método de segurança que exige duas ou mais formas diferentes de verificação para acessar um sistema, aumentando a proteção.

Backup: Cópia de segurança dos dados armazenados, utilizada para recuperação em caso de perda, falha ou ataque.

Classificação da Informação: Processo de categorizar as informações segundo seu grau de sensibilidade e criticidade, para definir níveis adequados de proteção.

Consentimento**:** Autorização clara e informada dada pelo titular para coleta e uso de seus dados pessoais.

Contingência: Plano de ações para resposta a falhas ou incidentes que possam afetar a continuidade das operações.

Dados Pessoais: Informações relacionadas a uma pessoa física, como nome, CPF, endereço, voz, entre outros.

Dados Pessoais Sensíveis**:** Dados pessoais que demandam proteção especial, como informações biométricas, saúde, orientação sexual ou opinião política.

Engenharia Social: Técnicas usadas para manipular pessoas a fim de obter informações confidenciais de forma fraudulenta.

Firewall: Sistema que monitora e controla o tráfego de dados entre redes, protegendo contra acessos não autorizados.

LGPD (Lei Geral de Proteção de Dados Pessoais): Legislação brasileira que regula a coleta, armazenamento, tratamento e compartilhamento de dados pessoais.

Menor Privilégio: Princípio que determina conceder a cada usuário apenas as permissões estritamente necessárias para realizar suas funções.

Phishing: Tentativa de fraude por meio de mensagens eletrônicas falsas que simulam comunicações legítimas para obter dados pessoais ou corporativos.

Plano de Continuidade de Negócios (PCN): Estratégia que garante a manutenção das atividades essenciais da organização em situações adversas.

Recursos de TI: Equipamentos, sistemas, redes e softwares disponibilizados pela organização para uso profissional.

Violação de Segurança: Qualquer ato ou evento que comprometa a confidencialidade, integridade ou disponibilidade das informações ou sistemas.

Diretrizes

Todas as atividades relacionadas ao uso e tratamento da informação devem observar os princípios abaixo:

- Toda informação da organização, em qualquer formato (físico ou digital), deve ser protegida contra acesso não autorizado, alteração, destruição, divulgação ou uso indevido.

Envio de comunicações eletrônicas:

O uso do e-mail corporativo deve ser restrito a comunicações relacionadas às atividades profissionais, visando preservar a integridade e confidencialidade das informações da organização. É expressamente proibido o envio de informações sensíveis ou confidenciais por e-mail sem a devida proteção, como criptografia ou uso de senhas, para evitar acessos não autorizados. Além disso, é fundamental que os colaboradores estejam atentos a tentativas de phishing e engenharia social, que buscam induzir o usuário a fornecer dados pessoais ou corporativos por meio de mensagens fraudulentas. A organização deve promover treinamentos periódicos para conscientizar os colaboradores sobre os riscos associados e as melhores práticas de segurança no uso de e-mails.

Classificação da informação:

Classificar as informações permite aplicar controles proporcionais à sensibilidade e ao potencial impacto que a divulgação, alteração ou perda dessa informação pode causar. As informações da organização devem ser classificadas de acordo com o seu grau de sensibilidade e criticidade para o negócio, conforme categorias abaixo:

Classificação	Definição	Exemplo
Pública	Informação que pode ser divulgada internamente e	Conteúdos institucionais, campanhas publicitárias, uma vez

	externamente sem restrição.	divulgadas pela organização
Interna	Informação de uso restrito aos colaboradores, que não deve ser divulgada externamente.	Comunicados internos.
Restrita	Informação crítica, de acesso extremamente limitado (interno ou externo). Um incidente com esse tipo de informação pode causar danos financeiros, jurídicos ou à reputação da organização.	Registros de investigações internas, processos disciplinares ou auditorias confidenciais.
Confidencial	Informação cujo acesso deve ser restrito a áreas e pessoas autorizadas. O vazamento, alteração ou uso indevido destes dados pode acarretar prejuízos financeiros, competitivos, legais ou comprometer a operação da organização	Dados de clientes, relatórios financeiros, estratégias comerciais.

Tratamento de dados pessoais:

Com relação ao tratamento de dados pessoais, a organização compromete-se a coletar, armazenar e tratar dados pessoais em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo a privacidade e os direitos dos

titulares. As diretrizes abaixo deverão ser seguidas em todas as áreas da organização:

- **Coleta e Tratamento:** os dados pessoais devem ser coletados e tratados apenas para finalidades legítimas, específicas e informadas ao titular, com base legal adequada e, quando necessário, mediante consentimento explícito.
- **Armazenamento Seguro:** todos os dados pessoais, incluindo gravações de chamadas, devem ser armazenados de forma segura, utilizando medidas técnicas e administrativas que protejam contra acessos não autorizados, vazamentos, alterações ou destruições acidentais ou ilícitas.
- **Acesso Restrito:** o acesso a dados pessoais ou dados pessoais sensíveis será restrito exclusivamente a pessoal autorizado, devidamente treinado e com necessidade comprovada para o desempenho de suas funções, conforme o princípio do menor privilégio.
- **Gravações de Chamadas:** as gravações de chamadas, por conterem dados pessoais e, potencialmente, dados sensíveis (como a voz, considerada dado biométrico), devem ser tratadas com especial atenção, assegurando-se o consentimento do titular quando aplicável e a adoção de medidas de segurança adequadas.

Política de senhas:

As senhas devem ser pessoais, intransferíveis e criadas com complexidade adequada, incluindo combinações de letras maiúsculas e minúsculas, números e caracteres especiais. Elas devem ser alteradas periodicamente, especialmente em casos de suspeita de comprometimento, e nunca devem ser compartilhadas com terceiros. Para reforçar a segurança, a organização deverá implementar autenticação multifator (MFA), adicionando uma camada extra de proteção ao exigir múltiplas formas de verificação de identidade.

Gestão de acessos:

A gestão de acessos é fundamental para proteger os ativos de informação da organização, garantindo que apenas usuários autorizados tenham acesso aos recursos necessários para desempenhar suas funções. Atribuições de acesso

devem ser feitas na organização com base no princípio do menor privilégio, assegurando que cada usuário possua apenas as permissões necessárias para suas atividades. As diretrizes abaixo devem ser seguidas:

- Os acessos devem ser concedidos de acordo com as responsabilidades do cargo, evitando privilégios excessivos.
- Deve ser feita avaliação regular os acessos concedidos, ajustando-os conforme mudanças nas funções ou estrutura organizacional.
- Desativar prontamente os acessos de colaboradores desligados ou transferidos para outras funções, prevenindo acessos não autorizados.
- Manter registros detalhados de concessões, alterações e revogações de acessos, sujeitos a auditorias internas periódicas.
- Limitar o acesso a dados pessoais ao mínimo necessário, conforme o princípio da minimização de dados estabelecido pela LGPD.
- Promover programas contínuos de treinamento para colaboradores sobre políticas de acesso e segurança da informação.

Segurança física das informações:

A segurança física é essencial para proteger os ativos da informação da organização contra acessos não autorizados, danos ou roubos. O controle de acesso físico às áreas restritas deve ser rigoroso, utilizando sistemas de reconhecimento como crachás, biometria ou outros mecanismos adequados para garantir que apenas pessoas autorizadas possam ingressar em locais sensíveis. Além disso, é fundamental implementar monitoramento por câmeras de segurança nas dependências da empresa, permitindo a vigilância contínua e a gravação de eventos para posterior análise, se necessário. A proteção contra incêndios, roubos e outros riscos físicos deve ser assegurada por meio de instalações adequadas, como extintores, alarmes e sistemas de detecção, além de treinamentos periódicos para os colaboradores sobre procedimentos de emergência.

Segurança lógica das informações:

A segurança lógica diz respeito à proteção dos sistemas de informação contra acessos não autorizados, alterações ou destruição de dados. A implementação de firewalls, antivírus e sistemas de detecção de intrusos (IDS) é fundamental para monitorar e controlar o tráfego de rede, identificando e prevenindo potenciais ameaças em tempo real. A criptografia de dados críticos, especialmente em comunicações entre matriz e filiais, deve ser aplicada para garantir a confidencialidade e integridade das informações durante a transmissão. Além disso, é imprescindível realizar backups regulares das bases de dados e sistemas, garantindo o armazenamento em locais seguros, para assegurar a recuperação das informações em caso de incidentes ou falhas técnicas.

Uso dos Recursos de TI

A utilização dos recursos tecnológicos, tais como computadores, sistemas e acesso à internet, é restrita exclusivamente a fins profissionais relacionados às atividades da organização. É expressamente proibida a instalação de softwares não autorizados pela área de TI, visando garantir a segurança, a integridade e o desempenho dos sistemas.

Utilização de dispositivos móveis:

É proibido o uso de dispositivos pessoais (BYOD) para assuntos corporativos sem autorização formal, garantindo que apenas aparelhos devidamente configurados e monitorados acessem recursos da organização. Todos os dispositivos móveis corporativos devem ser controlados e monitorados por meio de soluções de gerenciamento de dispositivos móveis, permitindo a aplicação de políticas de segurança, como criptografia, autenticação multifatorial e controle de aplicativos. Quando o acesso remoto for necessário, devem ser adotadas políticas específicas para garantir conexões seguras, incluindo o uso de VPNs, autenticação multifatorial e restrição de acessos conforme o princípio do menor privilégio.

Continuidade e contingência:

A organização deve implementar planos de contingência que abordem possíveis falhas técnicas, identificando riscos, estabelecendo procedimentos de resposta

e designando responsabilidades para assegurar uma recuperação eficiente. Além disso, a organização deve desenvolver um Plano de Continuidade de Negócios (PCN) abrangente, que contemple cenários de desastres tanto na matriz quanto nas filiais, garantindo a resiliência operacional em todas as unidades. A eficácia desses planos deve ser validada por meio de testes periódicos, como simulações de desastres e exercícios de mesa, para identificar falhas e aprimorar os procedimentos, assegurando que a organização esteja preparada para responder adequadamente a situações adversas.

Reporte de incidentes:

Qualquer violação ou suspeita de violação de segurança deverá ser comunicada imediatamente à área de Segurança da Informação. Após o reporte, serão imediatamente acionados os procedimentos de investigação e mitigação, conforme estabelecido no protocolo interno da organização, visando identificar a causa, conter os danos e evitar recorrências.

Treinamentos e conscientização:

A área de Segurança da Informação deve realizar treinamentos periódicos sobre segurança da informação para todos os colaboradores, incluindo analistas, gestores, estagiários e colaboradores terceirizados.

A abordagem deve ser contínua e adaptada às necessidades e ao perfil dos diferentes públicos, garantindo que todos estejam cientes dos riscos e das medidas preventivas relacionadas à segurança da informação.

Penalidades:

O não cumprimento das normas desta política sujeita o responsável a medidas disciplinares proporcionais à gravidade da infração. As sanções podem incluir advertência, suspensão e, em casos mais graves, desligamento. Além disso, poderá haver responsabilização legal conforme previsto na legislação vigente.

Revisão e atualização da Política

Esta política será revisada anualmente ou sempre que ocorrerem mudanças relevantes no ambiente tecnológico, organizacional ou legal.

Validade

Esta política entra em vigor na data de sua publicação e deve ser conhecida e assinada por todos os colaboradores, parceiros e terceiros que tenham acesso aos ativos de informação da empresa.

Responsabilidades

Diretoria:

- Apoiar e fiscalizar a implementação da PSI;
- Garantir a alocação de recursos financeiros, humanos e tecnológicos necessários para o cumprimento da política.
- Atuar como instância decisória em casos de incidentes de segurança da informação.

Gestores:

- Disseminar, aplicar e fiscalizar o cumprimento da PSI em suas equipes.
- Assegurar a aplicação e o cumprimento das diretrizes e procedimentos da PSI no ambiente sob sua responsabilidade.
- Identificar e reportar riscos e vulnerabilidades de segurança da informação à Área de TI e/ou Comitê de Segurança da Informação.

Área de Tecnologia da Informação:

- Garantir a segurança da infraestrutura tecnológica e suporte contínuo;
- Prover suporte técnico adequado, orientando gestores e demais colaboradores sobre procedimentos seguros e uso adequado dos recursos tecnológicos.

Área de Segurança da Informação:

- Definir, revisar e manter atualizada esta Política de Segurança da Informação (PSI).
- Implementar e manter controles técnicos e procedimentos para proteção contra ameaças, vulnerabilidades e incidentes de segurança.

- Investigar incidentes de segurança da informação, conduzindo o processo de resposta, registro e lições aprendidas.
- Atuar como ponto de contato para questões relacionadas à segurança da informação junto a órgãos reguladores, auditorias e demais partes interessadas.
- Auxiliar as áreas de negócio e a Área de TI na identificação e tratamento de riscos de segurança em novos projetos e novos sistemas.

Colaboradores:

- Cumprir integralmente as diretrizes e procedimentos estabelecidos;
- Manter o sigilo e a confidencialidade das informações às quais tiverem acesso durante o exercício de suas atividades;
- Reportar imediatamente quaisquer incidentes, suspeitas ou violações de segurança da informação à Área de SI;
- Participar de treinamentos e campanhas de conscientização promovidos pela empresa.