wikimeg

# PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Maio 2025

# SUMÁRIO

# MENSAGEM DA DIRETORIA

A SEGURANÇA É UM DOS ASSUNTOS E PREOCUPAÇÕES PRIORITÁRIAS DENTRE DA WIKIMEE. PORTANTO, NESSE DOCUMENTO APRESENTAREMOS UM CONJUNTO DE INSTRUÇÕES E PROCEDIMENTOS PARA NORMATIZAR E MELHORAR NOSSA VISÃO E ATUAÇÃO EM SEGURANÇA.

TODAS AS NORMAS AQUI ESTABELECIDAS SERÃO SEGUIDAS À RISCA POR TODOS OS FUNCIONÁRIOS, PARCEIROS E PRESTADORES DE SERVIÇOS. AO RECEBER ESTA CÓPIA DA POLÍTICA DE SEGURANÇA, VOCÊ SE COMPROMETE A RESPEITAR TODOS OS TÓPICOS AQUI ABORDADOS. A EQUIPE DE SEGURANÇA ENCONTRA-SE A TOTAL DISPOSIÇÃO PARA TIRAR DÚVIDAS E FORNECER AUXÍLIO TÉCNICO.

O NÃO CUMPRIMENTO DESSAS POLÍTICAS ACARRETARÁ EM SANÇÕES ADMINISTRATIVAS EM PRIMEIRA INSTÂNCIA, PODENDO ACARRETAR NO DESLIGAMENTO DO FUNCIONÁRIO DE ACORDO COM A GRAVIDADE DA OCORRÊNCIA.

# 1. OBJETIVO

A segurança da informação é um pilar fundamental para a continuidade e sucesso de nossa organização. Esta política reflete nosso compromisso em proteger nossos ativos digitais, garantir a confidencialidade, integridade e disponibilidade das informações, e cumprir com as legislações e regulamentações aplicáveis.

Entendemos que a segurança da informação é uma responsabilidade compartilhada entre todos os colaboradores, parceiros e partes interessadas. Portanto, esperamos que todos cumpram rigorosamente as diretrizes estabelecidas neste documento, adotando uma postura proativa na identificação e mitigação de riscos.

Estamos cientes de que as ameaças à segurança da informação são dinâmicas e em constante evolução. Assim, esta política será revisada e atualizada periodicamente para garantir que continue alinhada com as melhores práticas e com as necessidades da nossa organização. Contamos com a colaboração de todos para manter um ambiente seguro e resiliente, capaz de suportar os desafios e as mudanças no cenário digital.

Finalmente, reiteramos que qualquer incidente ou suspeita de violação de segurança deve ser imediatamente comunicada ao setor responsável, para que medidas adequadas possam ser tomadas. Somente com a colaboração e vigilância de todos, podemos assegurar a proteção e a confiança necessárias para o sucesso contínuo de nossa organização.

A Política de Segurança da Informação (PSI) é o documento que orienta e estabelece as diretrizes corporativas da WIKIMEE para a proteção dos ativos de informação e a prevenção da responsabilidade legal para todos os usuários. Deve, portanto, ser cumprida e aplicada em todas as áreas da instituição.

Esta política visa estabelecer princípios e orientar a definição de mecanismos de segurança que garantam o cuidado, a legalidade, a credibilidade e o prestígio do WIKIMEE na prestação dos seus serviços e, consequentemente, que preservem a continuidade dos seus negócios. Definir o escopo da segurança da informação no WIKIMEE e suas diretrizes para gerência e administração segura dos seus ativos e servir de referência para auditoria, apuração e avaliação de responsabilidades.

# 2. ABRANGÊNCIA

Esta Política foi elaborada conforme as Diretrizes de Compliance da WIKIMEE e estabelece regras de conduta que devem ser adotadas por todos aqueles que atuam em nome da WIKIMEE ou para ela, incluindo seus sócios, administradores, empregados, parceiros e colaboradores internos e externos, contratados e fornecedores.

A cópia desta Política e suas atualizações serão entregues em versão eletrônica ou impressa a todos os interessados. A versão eletrônica estará disponível também no site da WIKIMEE.

Após a leitura e compreensão desta Política, empregados, sócios, administradores e colaboradores devem assinar o "Termo de Conhecimento e Adesão" constante no Anexo I.

É condição obrigatória para a contratação de novos empregados ou colaboradores a assinatura do "Termo de Conhecimento e Adesão" constante no Anexo I.

# 3. SEGURANÇA DA INFORMAÇÃO

## 3.1. CONCEITOS E DEFINIÇÕES

Nesta Política são utilizadas as seguintes definições:

- Ameaça – causa potencial de um incidente de segurança, que pode resultar em dano para um ativo da instituição;
- Ativo – qualquer bem, tangível ou intangível, que possui valor para a instituição;
- Autenticidade – garantia da veracidade da fonte da informação;
- Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a pessoas, processos não autorizados;
- Cópia de segurança (backup) – imagem fiel de um ativo (documento, arquivo, sistema, outros) que possa ser restaurado em caso de impossibilidade de acesso ao original;

- Disponibilidade – propriedade da informação estar acessível para pessoas, sistemas e serviços autorizados, sempre que necessário;
- Evento de segurança da informação – ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da PSI ou falha de controles, ou uma situação previamente desconhecida que possa ser relevante para a segurança da informação;
- Gestor do ativo – membro da instituição responsável pela segurança de um determinado ativo;
- Incidente de segurança da infomação – ocorrência indicada por um único ou por uma série de eventos de segurança da informação indesejados ou inesperados, que apresentem grande probabilidade de comprometer as operações de negócio e ameaçar a segurança das informações no que tange a confidencialidade, integridade ou disponibilidade;
- Integridade - propriedade de salvaguarda da exatidão e completeza da informação. A certeza de que uma informação não foi modificada de forma não autorizada;
- Risco de segurança da informação - combinação entre a probabilidade de ocorrência de um incidente de segurança e as suas consequências;
- Segurança da Informação – preservação da confidencialidade, integridade e disponibilidade da informação que estão sob responsabilidade da instituição;
- Usuário – servidores, aposentados, discentes, terceirizados, colaboradores, consultores, auditores, agentes públicos, alunos, estagiários, bolsistas, pesquisadores, visitantes, empresas, organizações ou qualquer agente público que tenha o acesso aos ativos autorizados pelo responsável do ativo;
- Vulnerabilidade – fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

## 3.2. DISTRIBUIÇÃO E ATUALIZAÇÃO

A Política de Segurança da Informação deve ser de conhecimento de todos aqueles que atuam em nome da WIKIMEE ou para ela, incluindo seus sócios, administradores, empregados, parceiros e colaboradores internos e externos, contratados e fornecedores.

Está deverá ser revisada e atualizada a cada 1 ano após a sua publicação ou quando for identificada a necessidade pelo Comitê Executivo / Área de Segurança da Informação.

## 3.3. PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Os princípios que regem a segurança da informação e comunicação da WIKIMEE, no âmbito dos serviços, recursos e as informações relacionadas a:

- Autenticidade – propriedade de ser genuíno e apto a ser verificável e confiável;
- Confidencialidade – garantia que a informação esteja disponível, ou seja, revelada somente a usuários ou processo autorizados;
- Disponibilidade – a propriedade de um sistema ou recurso de estar acessível ou utilizável sob demanda do usuário;
- Integridade – a propriedade de assegurar que as informações não foram alteradas, perdidas ou destruídas de maneira não autorizada ou acidental;
- Legalidade – a propriedade de garantir a obediência aos princípios constitucionais, administrativos e à legislação vigente.
- Princípio da Eficiência dos Processos e Alcance dos Objetivos: A implementação de diretrizes e regras de segurança da informação deve permitir o pleno e seguro atendimento da missão da WIKIMEE, o alcance dos objetivos estratégicos e a operacionalização eficiente dos processos.
- Princípio do Acesso à Informação: As diretrizes, regras ou controles de segurança da informação não se sobrepõem ao Princípio da Publicidade que estabelece a necessidade da divulgação de informações para fins de transparência, prestação de contas e fiscalização. Ressalta-se que qualquer nível de restrição de acesso à informação deve estar amparado neste princípio, na legislação vigente e nas diretrizes a serem estabelecidas para a classificação da informação da WIKIMEE.

## 3.4. DIRETRIZES GERAIS

| Uso de e-mail | |
|---|---|
| | O e-mail da organização é ferramenta de comunicação e apenas como tal deve ser utilizada, sendo permitida sua utilização para fins pessoais, salientando que o uso é passível de auditoria e monitoramento e que deve ser utilizado com cautela, considerando as diretrizes contidas na PSI e demais normativos e principalmente a legislação vigente e a ética e desde que não infrinja as regras contidas nesta política, em suas normas complementares ou legislação aplicável.<br><br>Critérios para concessão de acesso ao e-mail, padrões de nomenclatura dos e-mails, período de retenção de mensagens e demais características do serviço devem ser definidas pela área de TI e serem comunicadas para a organização sempre que alguma mudança ocorrer e que possa afetar diretamente o usuário.<br><br>Não é permitida, em nenhuma circunstância, a divulgação dos endereços eletrônicos dos usuários da organização sem a devida anuência destes. |
| **A** | Não abra anexos com as extensões .exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf ou qualquer outra extensão que represente um risco à segurança; |
| **B** | Não envie e-mails do tipo corrente, compartilhamento de fake News, campanhas para crianças desaparecidas, pagamento de rifas, ou qualquer coisa que caracterize SPAM, etc, e uso indevido do e-mail; |
| **C** | Não utilize o e-mail da empresa para assuntos pessoais, sem devida autorização; |
| **D** | Não mande e-mails para mais de 10 pessoas de uma única vez. Utilize cc ou bcc; |
| **E** | Não divulgue informações não autorizadas ou imagens de tela, sistemas, documentos e afins sem autorização expressa e formal concedida pelo proprietário desse ativo de informação, assim como não compartilhar informações pessoais dos clientes; |
| **F** | Não falsifique informações de endereçamento, adulterar cabeçalhos para esconder a identidade de remetentes e/ou destinatários, com o objetivo de evitar as punições previstas; |
| **G** | Não produza, transmita ou divulgue mensagens que tenham conteúdo considerado impróprio, obsceno ou ilegal; |
| **H** | Não será tolerado e-mails contendo perseguição preconceituosa baseada em sexo, raça, incapacidade física ou mental ou outras situações protegidas; |
| **I** | Os e-mails sempre devem conter seu nome, telefone, logotipo e área da empresa; |
| **J** | Não cadastre o e-mail institucional em listas de discussões não ligadas ao trabalho. |

| Acesso à Internet | |
|---|---|
| | O acesso à Internet da WIKIMEE deve ser regido por norma específica, atendendo às determinações desta PSI, e demais orientações governamentais e legislação em vigor, com utilização exclusiva para fins de complementação às suas atividades, para o enriquecimento intelectual ou como ferramenta de busca por informações que venham a contribuir para o desenvolvimento de seus trabalhos.<br>Todo o conteúdo acessado pelos usuários poderá ser monitorado e gravado para futuras averiguações.<br>O uso da Internet para fins pessoais é permitido conforme orientação do gestor. É proibido acessar sites com conteúdo relacionado a crimes, drogas, pornografia, pedofilia, racismo, difamação, entre outros.<br>O uso da Internet para fins pessoais não é permitido. |
| **A** | Sites com conteúdo pornográfico, jogos, download de filmes, músicas, torrent, bate-papo, softwares piratas, conteúdos nocivos com vírus/malwares, apostas e similares não devem ser acessados a partir do escritório da empresa; |
| **B** | Não utilize os recursos da empresa para deliberadamente propagar qualquer tipo de vírus, worm, trojan, spam, assédio, perturbação ou software de controle de outros computadores; |
| **C** | Materiais de cunho sexual não podem ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso. |

| Tratamento da Informação | |
|---|---|
| **A** | Toda informação sob responsabilidade da WIKIMEE é considerada um bem e deve ser protegida de acordo com as diretrizes descritas nesta PSI, normas e demais regulamentações em vigor, com o objetivo de minimizar os riscos que afetem os requisitos de segurança das informações e preservando a imagem da instituição.<br>As informações críticas devem possuir cópia de segurança atualizada e essa cópia deve ser testada periodicamente. |
| **B** | Deve-se implementar procedimentos para tratamento, armazenamento, identificação, classificação e descarte das informações da WIKIMEE para assegurar a integridade, disponibilidade e confidencialidade das informações.<br>As regras para as operações de armazenamento, divulgação, reprodução e destruição da informação devem ser definidas na norma de classificação da informação. |
| **C** | As informações críticas devem possuir cópia de segurança atualizada e essa cópia deve ser testada periodicamente. |

| NDA (“Non Disclosure Agreement”), ou Acordo de Não Divulgação | |
|---|---|
| **A** | Todas informações estratégicas e confidenciais não devem ser divulgadas a terceiros, sem devida autorização e devem seguir as práticas conforme a classificação das mesmas.<br><br>Também não é permitido divulgação das mesmas, de forma a comprometer as políticas de Segurança da WIKIMEE e também de seus clientes e parceiros, assim como todo o software está protegido pela legislação pertinente a propriedade industrial, ao direito autoral e ao sigilo de negócios de fabricação e é de propriedade exclusiva da WIKIMEE que detém todos os direitos sobre o mesmo. |
| **B** | A propriedade intelectual, titularidade e todos os direitos autorais referentes ao SOFTWARE e seu CÓDIGO-FONTE (incluindo, mas sem limitação a quaisquer imagens, fotografias, animações, vídeos, áudios, músicas, textos, componentes e arquivos incorporados, documentação e quaisquer cópias do software) que são de propriedade exclusiva da WIKIMEE. |
| **C** | É terminantemente proibido, reproduzir, distribuir, alterar, vazamento de código-fonte, publicação do código completo, ou de trechos em repositórios ou fóruns públicos, utilizar engenharia reversa ou valer-se de qualquer tentativa de reverter ao seu código-fonte qualquer dos componentes que compõe o SOFTWARE para revenda, pirataria, reutilização, criação de SOFTWARE similar à terceiros e/ou concorrentes ou agir de má fé. |
| **D** | O não cumprimento deste termo de sigilo acarretará todos os efeitos de ordem penal, civil e administrativa, rescisão de contrato, multas, indenização e ações cabíveis, assumindo as respectivas responsabilidades. |
| **E** | É dever de todos Colaboradores e parceiros zelar pelo sigilo e propriedade intelectual da WIKIMEE. |

| Controle de Acesso Lógico | |
|---|---|
| **A** | O acesso à informação será regulamentado por normas específicas onde toda e qualquer informação gerada, adquirida, utilizada ou armazenada pela organização é considerada seu patrimônio e deve ser passível de proteção e monitoramento. |
| **B** | As regras de controle de acesso a todos os sistemas da instituição deverão ser definidos e regulamentados, através de norma a ser desenvolvida, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da WIKIMEE<br><br>Todo acesso às informações deve ser controlado de forma a garantir que apenas pessoas autorizadas, pelo respectivo proprietário da informação, tenham acesso. |
| **C** | A gestão de acessos a informação deverá obedecer ao princípio de menor privilégio possível, podendo os usuários terem acesso à não mais do que as informações e recursos computacionais necessários para o pleno desenvolvimento de suas atividades.<br><br>As credenciais de acesso concedidas aos usuários são pessoais e intransferíveis, podendo seu uso ser auditado e monitorado, não devendo o usuário conceder suas credenciais a terceiro sob quaisquer circunstâncias.<br><br>Visitantes que necessitarem acessar à Internet, porém, poderão fazê-lo por meio de solicitação formal, devidamente autorizada pelo gestor da área visitada, com período de acesso previamente definido. |

| Controle de Acesso Físico e proteção do perímetro | |
|---|---|
| **A** | O acesso às dependências da organização deve ser controlado e monitorado. O porte e uso das devidas credenciais de acesso, as quais são pessoais, únicas e intransferíveis, devendo estas permitir de maneira clara e inequívoca o reconhecimento de seu detentor.<br><br>Os ativos de TI da WIKIMEE devem ser mantidos em áreas seguras, protegidos por um perímetro de segurança, com barreiras apropriadas e recursos para controle de acesso conforme regras a serem estabelecidas em norma específica sobre o tema. |
| **B** | As instalações físicas, estações de trabalho, servidores, softwares e demais equipamentos de TIC da WIKIMEE devem ser protegidos contra acessos indevidos e riscos de indisponibilidade.<br><br>Os servidores devem ser mantidos em áreas protegidas por controle de acesso, conforme regras a serem definidas em norma |
| **C** | A instituição deve implementar controles para monitorar o acesso físico ao ambiente, equipamentos, documentos de modo que a segurança seja mantida, restringindo o acesso a apenas usuários autorizados, as regras e controles devem ser definidos e norma específica sobre o tema.<br><br>Locais considerados críticos devem possuir métodos de controle de acesso rígido, de modo que somente pessoas autorizadas e acompanhadas possam ter acesso. Os acessos devem ser registrados e as autorizações devem ter tempo determinado, o controle de acesso deve ser preferencialmente de forma eletrônica, através de biometria ou cartões de acesso e senha. |

| Engenharia Social | |
|---|---|
| | Ataque de engenharia social é uma técnica de manipulação psicológica usada por cibercriminosos para enganar indivíduos e levá-los a divulgar informações confidenciais, realizar ações inseguras ou conceder acesso a sistemas protegidos. Ao contrário dos ataques técnicos, que exploram falhas de software ou hardware, a engenharia social explora fraquezas humanas, como a confiança, curiosidade, medo ou pressa.<br><br>Portanto cabe a todos envolvidos se atentarem as diretrizes de prevenção, e em caso de suspeita de ataques de estelionato, engenharia social, o time de segurança da informação deverá ser relatado imediatamente. |
| **Educação e Treinamento** | • **Programas de Conscientização:** Implementar treinamentos regulares para todos os funcionários sobre os diferentes tipos de ataques de engenharia social, como phishing e outros ataques de falsidade ideológica.<br>• **Links e e-mails suspeitos:** Implementar treinamentos regulares para todos os funcionários sobre a importância de não clicar em links e e-mails suspeitos, e sempre relatar ao time de segurança, caso de suspeita de fraude ou ataque.<br>• **Simulações de Ataques:** Realizar simulações periódicas de ataques de engenharia social, como campanhas de phishing internas, para testar a conscientização dos funcionários e melhorar as práticas de segurança.<br>• **Reconhecimento de Técnicas de Manipulação:** Ensinar os funcionários a reconhecer técnicas comuns de manipulação emocional ou psicológica que os atacantes utilizam para ganhar confiança ou pressionar decisões rápidas. |
| **Procedimentos de Verificação** | • **Verificação de Identidade**: Exigir a verificação rigorosa de identidade para qualquer solicitação que envolva informações sensíveis ou acesso a sistemas críticos, incluindo a confirmação de identidades através de múltiplos canais (ex.: telefone e e-mail).<br>• **Confirmação de Solicitações**: Estabelecer políticas que requerem a confirmação de solicitações de mudanças de senha, transferências financeiras ou fornecimento de informações confidenciais por meio de um segundo fator de autenticação ou |
| **Gestão de Informações** | • **Confidencialidade de Dados**: Reforçar a importância de proteger informações confidenciais, como credenciais de login, números de identificação e dados financeiros, e evitar compartilhá-las por canais não seguros.<br>• **Compartilhamento de Informações**: Implementar práticas que limitem o compartilhamento de informações sensíveis, especialmente via e-mail, telefone ou outros meios eletrônicos, a menos que seja absolutamente necessário e que o destinatário tenha sido devidamente verificado. |
| **Políticas de Comunicação** | • **Uso de Comunicação Oficial**: Exigir que todas as comunicações sensíveis, como solicitações de informações financeiras ou pessoais, sejam realizadas por meio de canais oficiais da empresa, com protocolos de segurança apropriados.<br>• **Atenção a Solicitações Incomuns**: Instruir os funcionários a ficarem atentos a solicitações incomuns, urgentes ou que não sigam os procedimentos habituais, e a confirmar essas solicitações diretamente com a pessoa supostamente envolvida antes |

| | |
|---|---|
| **Monitoramento e Resposta** | • **Monitoramento de Tentativas de Engenharia Social**: Implementar sistemas que possam detectar e alertar sobre possíveis tentativas de engenharia social, como acesso repetido a sistemas sem sucesso ou padrões incomuns de solicitação de informações.<br>• **Procedimentos de Relato**: Estabelecer um canal de comunicação seguro e acessível para que os funcionários possam relatar |
| **Política de Manuseio de Incidentes** | • **Resposta a Incidentes**: Desenvolver um plano de resposta para incidentes específicos de engenharia social, detalhando os passos a serem seguidos se um ataque for detectado, incluindo a notificação de partes relevantes e a implementação de contramedidas.<br>• **Análise Pós-Incidente**: Após qualquer incidente de engenharia social, realizar uma análise detalhada para identificar falhas no |
| **Proteção de Informação Pública** | • **Limitação de Informação Disponível Publicamente:** Minimizar a quantidade de informações sensíveis ou pessoais que estão disponíveis publicamente (por exemplo, nas redes sociais corporativas ou websites) para reduzir as oportunidades de coleta de dados por engenheiros sociais.<br>• **Política de Redes Sociais**: Estabelecer diretrizes sobre o que os funcionários podem ou não compartilhar nas redes sociais, particularmente informações que possam ser utilizadas para personalizar ataques de engenharia social. |

| **Malware / Vírus e Software Malicioso** | |
|---|---|
| | Fica vetado o uso de software maliciosos que possam comprometer a segurança de quaisquer ativos da Wikimee, assim como acesso a sites maliciosos e que potencialmente ofereçam riscos que possam comprometer a segurança.<br>E cabe a todos envolvidos se atentarem nas diretrizes mitigatórias e preventivas contra este tipo de ameaça.<br>Também é importante a notificação de atividades suspeitas relacionadas a softwares, em caso de suspeita de infecção por malware, links suspeitos, tentativas de phishing, o time de segurança deve ser imediatamente notificado para investigação, mitigação e tratativa do mesmo. |
| **Proteção** | • **Uso de Antimalware**: Instalar e manter atualizado software antimalware em todos os dispositivos e servidores da organização.<br>• **Escaneamento Regular**: Realizar escaneamentos regulares em todos os sistemas para detectar e remover possíveis ameaças de malware.<br>• **Monitoramento de Comportamento**: Implementar soluções de segurança que monitoram o comportamento dos programas para identificar atividades suspeitas ou maliciosas. |

| | |
|---|---|
| **Atualização e Patching** | • **Manutenção de Software**: Garantir que todos os sistemas operacionais, aplicativos e softwares de segurança sejam mantidos atualizados com os últimos patches de segurança.<br>• **Correção de Vulnerabilidades**: Implementar um processo rápido para aplicar patches e correções em sistemas que apresentem vulnerabilidades conhecidas exploradas por malware. |
| **Gestão de Dispositivos** | • **Controle de Dispositivos Externos**: Restringir o uso de dispositivos externos (como USBs e discos rígidos) e implementar políticas para escanear automaticamente qualquer dispositivo antes do uso.<br>• **Segmentação de Rede**: Segmentar a rede para limitar a propagação de malware entre diferentes partes da organização. |
| **Educação e Conscientização** | • **Treinamento sobre Malware**: Oferecer treinamentos regulares para funcionários sobre como identificar sinais de malware e práticas seguras para evitar infecções.<br>• **Política de Downloads**: Educar os funcionários sobre os perigos de baixar software ou abrir anexos de fontes não confiáveis. |
| **E-mail e Navegação Segura** | • **Filtragem de E-mails**: Utilizar filtros de e-mail para bloquear anexos suspeitos e links que possam conter malware.<br>• **Navegação Restrita**: Implementar políticas de filtragem de web para bloquear o acesso a sites conhecidos por distribuir malware. |
| **Monitoramento e Resposta** | • **Monitoramento Contínuo**: Implementar sistemas de monitoramento em tempo real para detectar atividades anômalas indicativas de malware.<br>• **Plano de Resposta a Incidentes**: Desenvolver e testar um plano de resposta específico para incidentes de malware, incluindo procedimentos de contenção, erradicação e recuperação. |
| **Backup e Recuperação** | • **Backups Seguros**: Realizar backups regulares de dados críticos e garantir que esses backups sejam armazenados em locais isolados, protegidos de ataques de malware, como ransomware.<br>• **Testes de Recuperação**: Testar regularmente a capacidade de recuperação de dados a partir de backups em caso de infecção por malware. |
| **Controle de Acesso** | • **Privilégios Mínimos**: Adotar o princípio do menor privilégio, garantindo que os usuários tenham apenas as permissões necessárias para desempenhar suas funções, reduzindo o risco de disseminação de malware.<br>• **Isolamento de Contas Comprometidas**: Implementar procedimentos para isolar rapidamente contas comprometidas que possam estar espalhando malware dentro da rede. |

| Equipamentos Pessoais - BYOD | |
|---|---|
| | As diretrizes para a utilização de dispositivos pessoais (Bring Your Own Device - BYOD) pelos colaboradores e parceiros da Wikimee, devem garantir a segurança da informação e a proteção dos dados corporativos acessados e armazenados em tais dispositivos.<br><br>Estes equipamentos devem estar em conformidade com as políticas de segurança da informação da Wikimee, bem como com as normas e regulamentações aplicáveis, tais como:<br><br>• ISO/IEC 27001 - Gestão de Segurança da Informação: estabelece os requisitos para um sistema de gestão da segurança da informação, incluindo aspectos relacionados ao BYOD.<br><br>• ISO/IEC 27002 - Código de Práticas para Controles de Segurança da Informação: fornece diretrizes para a implementação de controles de segurança, aplicáveis ao uso de dispositivos pessoais.<br><br>• Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018: regula o tratamento de dados pessoais e deve ser estritamente observada no uso de dispositivos BYOD.<br><br>O não cumprimento das diretrizes estabelecidas neste termo poderá resultar em sanções, incluindo, mas não se limitando a restrições de acesso aos sistemas corporativos, rescisão de contratos e/ou responsabilidade por eventuais danos causados à Wikimee ou a |
| **A** | **Proteção por senha:** O dispositivo deve ser protegido por senha forte ou outro mecanismo de autenticação seguro. |
| **B** | **Criptografia de dados**: Todos os dados corporativos armazenados no dispositivo devem ser criptografados para prevenir acessos não autorizados. |
| **C** | **Atualizações de software**: O sistema operacional e os aplicativos instalados no dispositivo devem estar sempre atualizados com as últimas versões e patches de segurança. |
| **D** | **Antivírus e firewall**: O dispositivo deve possuir softwares de proteção como antivírus e firewall devidamente configurados e |
| **E** | **Acesso controlado**: O acesso aos dados corporativos só deve ser realizado por meio de conexões seguras, como VPN, e deve ser restrito conforme as políticas da Wikimee. |

| Autenticação e Segundo Fator de Autenticação (2FA) | |
|---|---|
| **Autenticação** | A autenticação nos sistemas de informática geralmente é baseada em uma senha. Esse meio é muito utilizado por sua facilidade de implantação e manutenção e por seu baixo custo. Porém, é um meio inseguro e suscetível à ataques. Por isso foi criada a autenticação de dois fatores (2FA), um meio que exige que o usuário forneça dois meios de identificação antes de conseguir se autenticar. |
| **2FA** | Autenticação por dois fatores, também conhecida como 2FA, é uma informação adicional que é usada para permitir acesso à determinado serviço. Normalmente as pessoas somente utilizam um nome de usuário e uma senha. Mas se a senha é fácil de adivinhar ou foi roubada, a conta poderia ficar comprometida. Ela oferece identificação aos usuários através da combinação de dois componentes diferentes. Esses componentes podem ser algo que o usuário sabe, algo que o usuário possui ou algo que é inseparável do usuário. Um bom exemplo da vida cotidiana é a operação de saque em um terminal bancário de autoatendimento. Apenas a combinação correta do cartão (algo que o usuário possui) e da senha (algo que o usuário sabe) permite a operação ser completada.<br><br>É considerada uma boa prática o uso da autenticação por dois fatores quando ela estiver disponível. |

| Senhas | |
|---|---|
| | Para facilitar a memorização das senhas, utilize padrões mnemônicos. As senhas devem ter um tempo curto de vida útil, devendo ser alteradas com periodicidade: Não é permitida, em nenhuma circunstância, a divulgação dos endereços eletrônicos dos usuários da organização sem a devida anuência destes. Utilize sempre senhas fortes para evitar que a mesma seja descoberta por terceiros e |
| **A** | Utilize senhas de no mínimo 8 caracteres, alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação de maiúsculo e |
| **B** | Não utilize a mesma senha para diversas finalidades, por exemplo, para sistemas corporativos, conta bancária, e-mail, etc. |
| **C** | Sua senha é **intrasferível** e não deve ser jamais passada a ninguém. Caso desconfie que sua senha não está mais segura, você deve altera-la imediatamente; |
| **D** | Tudo que for executado com a sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para manter sua senha secreta; |
| **E** | As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos não criptografados; |
| **F** | As senhas 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<br><br>devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras; |
| **G** | Utilize um software gerenciador de senhas para gerar senhas fortes e armazena-las de forma segura. |

| Segurança em Recursos Humanos | |
|---|---|
| **A** | Os usuários, parceiros e colaboradores da WIKIMEE devem ter ciência de suas responsabilidades e obrigações relacionadas a PSI e demais normativos complementares, assim como cumprir está política.<br><br>Devem ser estabelecidos processos e procedimentos relacionados a disseminação da cultura em segurança da informação, ao ciclo de vida dos usuários da instituição e responsabilidades atreladas a cada processo. |
| **B** | WIKIMEE deve definir regras, em normativo específico, no que diz respeito ao ciclo de vida dos usuários na instituição desde a contratação/início das atividades até o desligamento/término do contrato, incluindo as movimentações e promoções, como também o processo de coleta do termo de ciência / responsabilidade em relação à está política e demais normativos.<br><br>Deve prever como será a disseminação da cultura de segurança da informação na WIKIMEE. |
| **C** | As responsabilidades em relação à segurança da informação devem ser comunicadas na fase de contratação dos colaboradores e parceiros. Estes devem ser orientados a seguir as diretrizes desta política e de suas normas complementares, assinando um termo de ciência que deverá ficar de posse do departamento pessoal.<br><br>É responsabilidade do gestor do colaborador ou do contrato, em conjunto com o departamento pessoal, informar a área de TI sobre o desligamento de um colaborador, parceiro ou término de um contrato para que as credenciais de acesso sejam devidamente revogadas.<br><br>Como forma de manter todos atualizados quanto às normas de segurança da informação, é responsabilidade da WIKIMEE, implementar um plano de treinamentos e conscientização permanente na organização, inclusive avaliando a eficácia destes |

| Gestão de incidentes de segurança | |
|---|---|
| **A** | Os incidentes de segurança da informação devem ser identificados, registrados, tratados e monitorados. As regras e controles devem ser definidos em norma e processo específico sobre o tema.<br><br>Os colaboradores, parceiros e usuários devem ser estimulados a reportar os incidentes, atividades ou comportamentos suspeitos, assim como o não cumprimento desta política e demais normativos de segurança da informação por meio dos canais de comunicação da WIKIMEE. |
| **B** | Na WIKIMEE, uma equipe deverá receber, filtrar, classificar, analisar e responder os incidentes de segurança conforme regras definidas em norma específica para o tema. |
| **C** | Todo e qualquer incidente de segurança da informação deve ser comunicado imediatamente. Os incidentes devem ser identificados, registrados, respondidos e monitorados por uma equipe capacitada para este fim através de um processo formal e de conhecimento de toda a organização. |

| Gestão de Riscos de Segurança da Informação | |
|---|---|
| **A** | A WIKIMEE deve estabelecer um processo de Gestão de Risco de Segurança da Informação contínuo e estruturado.<br><br>Os riscos de segurança da informação devem ser monitorados e analisados periodicamente, a fim de verificar mudanças nos critérios de avaliação e aceitação dos riscos, no ambiente, nos ativos de informação e em fatores de risco, como ameaça, vulnerabilidade, probabilidade e impacto. |
| **B** | Este processo deve ser implementado e mantido visando minimizar impactos nos processos da WIKIMEE, parceiros e principalmente seus clientes.<br><br>Os ativos de informação a serem protegidos deverão ser priorizados, de acordo com o mapa de risco, bem como a definição e implantação de controles para a o tratamento dos riscos. |
| **C** | Os riscos relativos à informação devem ser gerenciados de modo a reduzir vulnerabilidades e impactos referentes aos ativos de informação.<br><br>A gestão de riscos de segurança da informação deve ser implementada por meio de planejamento de segurança fundamentado em desenvolvimento de cultura corporativa para riscos, qualificação de pessoas, desenvolvimento de procedimentos e implantação de tecnologia e recursos. |

| Gestão de Continuidade dos Negócios | |
|---|---|
| **A** | O processo de gestão de continuidade de negócios deve ser desenvolvido para gerenciar e manter em funcionamento os serviços e processos críticos da WIKIMEE, na ocorrência de desastres, falhas ou incidentes.<br><br>Os planos devem ser desenvolvidos com base na análise de riscos de segurança da informação. |
| **B** | O processo de gestão da continuidade de negócios deve ser implementado, mantido e testado periodicamente visando reduzir, para um nível aceitável, o tempo de interrupção causado por um desastre ou falhas nos recursos que suportam os ativos da organização. |
| **C** | A WIKIMEE deve manter planos de continuidade de negócios, atualizados e testados periodicamente, a fim de evitar que os processos e atividades críticas sejam interrompidas por um desastre ou incidente. A instituição deve estabelecer as regras para a continuidade dos negócios em norma específica. |

### 3.5. RESPONSABILIDADES

| | |
|---|---|
| Clientes, Usuários, Colaboradores e Parceiros da WIKIMEE | • Desenvolver as suas atividades seguindo as diretrizes e definições da Política de Segurança da Informação e Comunicação (PSI) e demais normativos relacionados ao tema;<br>• Assinar o termo de responsabilidade para o uso dos recursos tecnológicos da instituição (quando aplicável);<br>• Reportar os incidentes de segurança através dos meios divulgados pela instituição;<br>• Ter ciência, compreender e aplicar as diretrizes e regras estabelecidas na PSI;<br>• Tratar as informações como patrimônio da WIKIMEE, e como tal, preservar pela confidencialidade, disponibilidade e integridades das informações, não divulgando para pessoas não autorizadas;<br>• Não compartilhar, transferir, divulgar ou permitir o conhecimento das suas credenciais e senhas a outros usuários. |
| Chefia da WIKIMEE | • Gerenciar o cumprimento da PSI e demais da WIKIMEE por parte de seus subordinados;<br>• Identificar os desvios praticados e adotar medidas corretivas, quando necessário;<br>• Proteger, em nível físico e lógico, os ativos que estão sob a sua responsabilidade;<br>• Garantir que os usuários sob a sua responsabilidade receberam o devido treinamento em relação à segurança da informação e comunicação;<br>• Aplicar, quando necessário, em conjunto com a área de pessoal as medidas disciplinares, conforme legislação vigente;<br>• Autorizar o acesso as informações sob sua responsabilidade;<br>• Requisitar auditoria nos processos envolvidos com a PSI no intuito de aferir o nível de segurança da informação, violações de segurança e não conformidades;<br>• Classificar as informações quanto à confidencialidade no momento em que a informação for produzida ou obtida. |
| Responsável pelo Departamento Pessoal | • Apoiar na aplicação de sanções disciplinares;<br>• Obter dos usuários a assinatura do termo de ciência / responsabilidade;<br>• Apoiar no processo de disseminação da cultura em segurança da informação, quando aplicável;<br>• Definir, nas descrições de cargos e funções, as responsabilidades dos servidores pela manutenção das ações de segurança da informação e comunicação;<br>• Promover a ambientação / integração de todo servidor, por meio de treinamento e capacitação no tema segurança da informação e comunicação. |

| | |
|---|---|
| Comitê de Segurança da Informação | O Comitê de Segurança da Informação é composto pelos seguintes membros:<br>1. Gestor de Segurança da Informação;<br>2. Sócios administradores da Wikimee;<br>3. Um membro Sênior da Equipe de Desenvolvimento de Produto<br><br>O Comitê de Segurança da Informação é responsável por realizar o constante monitoramento do Programa de Integridade, garantindo o cumprimento das normas previstas neste Código:<br>• Propor o desenvolvimento de Normas e Procedimentos relativos à segurança da informação e comunicações na instituição;<br>• Apresentar proposta de revisão da PSI e demais normativos, de forma a mantê-los sempre atualizados e de acordo com a legislação vigente;<br>• Assessorar a reitoria / diretoria geral nos assuntos relativos a segurança da informação e comunicação;<br>• Construir grupos de trabalho para tratar temas e propor soluções específicas sobre Segurança da Informação e Comunicações;<br>• Elaborar proposta e promover um Plano de Gestão de Riscos que inclua um Plano de Gestão de Incidentes de Segurança da Informação e um Plano de Continuidade de Negócio, com medidas que garantam a continuidade das atividades da WIKIMEE em caso de desastre ou falhas nos recursos que suportam os processos vitais de negócio.<br>• Analisar os casos não previstos neste Documento e solucionar as dúvidas sobre a sua aplicação.<br>• Promover treinamentos periódicos sobre ética e integridade entre os profissionais da Wikimee.<br>• Sugerir revisões e atualizações deste Documento à Diretoria da empresa, para garantir o seu constante aprimoramento.<br>• Aplicar as medidas disciplinares cabíveis às violações deste Documento após a apuração do fato pelo Gestor de Segurança da Informação.<br>• Apurar denúncias que indiquem, com elementos mínimos de veracidade, o envolvimento do Gestor de Segurança da |

| | |
|---|---|
| Gestor de Segurança da Informação | • Presidir o Comitê de Segurança da Informação;<br>• Promover a disseminação da cultura de segurança da informação e comunicação na instituição;<br>• Atuar na investigação e tratamento de incidentes de segurança da informação;<br>• As denúncias que indiquem supostas violações a este Documento serão recebidas pelos sócios administradores da Wikimee e repassadas ao Gestor de Segurança da Informação<br>• O Gestor da Segurança da Informação, designado pela Diretoria da Wikimee, será responsável pela apuração das denúncias, observadas as disposições previstas sobre o procedimento de investigação.<br>• Propor recursos necessários para as ações de segurança da informação;<br>• Manter o sistema normativo de segurança da informação e comunicação sempre atualizado, mantendo a melhoria contínua; |
| Diretoria Geral | • Aprovar a PSI e demais normativos relacionados à segurança da informação e comunicação;<br>• Promover a disseminação da cultura de segurança da informação e comunicação na instituição;<br>• Prover os recursos necessários para a implementação dos controles e ações de segurança da informação e comunicação na instituição;<br>• Indicar, orientar e autorizar, a qualquer tempo, procedimentos que visem garantir a segurança da informação, nos processos e documentos de sua competência, a serem seguidos pelos gestores da informação pertinentes. |

## 3.6. MONITORAMENTO E AUDITORIA

| | |
|---|---|
| **A** | O cumprimento da PSI e demais normativos relacionados à segurança da informação e comunicação da WIKIMEE devem ser auditados pela área de Segurança da Informação.<br><br>A WIKIMEE poderá monitorar os acessos dos usuários, incluindo o acesso à internet e uso do correio eletrônico, conforme necessidade e aprovação do gestor imediato. |
| **B** | Para efeitos de verificação do cumprimento das diretrizes e regras de segurança da organização a WIKIMEE poderá monitorar os acessos dos usuários aos sistemas corporativos, e-mail e à Internet, mediante decisão e autorização da <Reitoria/Alta Gestão>.<br><br>O cumprimento da PSI e das normas deverá ser avaliado a cada <X anos> por meios de auditorias de conformidade, conforme regras a serem estabelecidas em norma específica sobre o tema. |
| **C** | A WIKIMEE irá monitorar, automaticamente, todos os acessos dos usuários aos sistemas de seus sistemas.<br><br>Deve ser realizada, periodicamente, verificação de conformidade das práticas de segurança da informação da WIKIMEE com a PSI, normas, processos e procedimentos complementares, bem como com a legislação vigente.<br><br>É vedado aos usuários realizar a condução de verificação de conformidade dos processos aos quais está envolvido ou vinculado. |

## 3.7. SANÇÕES DISCIPLINARES

| | |
|---|---|
| **A** | A não observância das diretrizes da PSI da WIKIMEE pode acarretar, isoladamente ou cumulativamente, nos termos da legislação vigente em sanções administrativas, civis e/ou penais. |
| **B** | O descumprimento ou violação pelos colaboradores, parceiros, usuários das diretrizes previstas na PSI ou nos normativos poderá resultar na aplicação de punições previstas nos regulamentos internos, em sanções administrativas ou na legislação em vigor. |
| **C** | A violação da PSI da WIKIMEE e demais normativos relacionados à segurança da informação e comunicação poderá resultar em ação disciplinar, apoiada na legislação vigente e regulamentos internos.<br><br>Estando sujeitos ao regime jurídico, podem ser listadas nas penalidades aplicáveis, a saber:<br><br>I. advertência;<br><br>II. suspensão;<br><br>III. demissão;<br><br>IV. multas;<br><br>E em casos mais graves leis criminais aplicáveis. |

# 4. REFERÊNCIAS

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistema de gestão de segurança da informação – Requisitos;

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação;

Lei nº 13.709/2018 (Lei Geral de Proteção de Dados);

Norma complementar nº 03/IN01/DSIC/GSIPR de 3 de julho de 2009 – Departamento de Segurança da Informação e Comunicações.

# 5. ANEXO I: TERMO DE CONHECIMENTO E ADESÃO

Declaro ter lido e compreendido esta Política de Segurança da Informação a qual representa um código de conduta e assumo o compromisso de observá-lo e cumpri-lo integralmente em todas as minhas atividades relacionadas à empresa.

Tenho ciência de que o descumprimento das normas expostas neste documento estará sujeito às medidas disciplinares de caráter administrativo, cível, trabalhista e criminal e a eventuais sanções determinadas pela empresa conforme o instrumento contratual de vínculo com a Plataforma Digital Wikimee Ltda.

[Nome completo do declarante]

[Assinatura do declarante]

[Data]

wikimeo

# PSI - POLÍTICA DE SEGURANÇA DA INFORMAÇÃO