Política de Segurança da Informação

tecnoAtiva Consultoria e Sistemas LTDA.

Sumário

1. Objetivos

Estabelecer diretrizes aplicáveis à utilização das informações da tecnoAtiva e daquelas sob sua custódia, definindo controles de segurança necessários e adequados para minimizar a exposição das informações mencionadas a riscos.

2. Abrangência

Esta Política de Segurança da Informação se aplica a todos os usuários, fornecedores, parceiros ou indivíduos que acessem informações (digitais ou não) e os ativos de informação da tecnoAtiva ou de qualquer pessoa física ou jurídica sob custódia da tecnoAtiva.

3. Vigência

Essa política passa a vigorar a partir da data da publicação.

4. Conceitos e Definições

Os termos e definições a seguir são importantes para a compreensão desta Política de Segurança da Informação:

Ameaça: Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.

Ativo: Tudo que tem valor para a organização.

Ativos de informação: Conhecimentos ou dados que têm valor para o indivíduo ou para a organização.

Confidencialidade: Garantir que as informações sejam acessadas somente por aqueles expressamente autorizados, devendo ser protegidas do conhecimento alheio.

Integridade: Garantir que as informações estejam protegidas de modificações, manipulações ou reproduções não autorizadas.

Disponibilidade: Garantir que todas as informações e serviços importantes ao negócio estejam disponíveis, sempre que necessário, a pessoas e processos autorizados.

Controle: É uma medida de segurança que modifica o risco. Os controles são implementados para mitigar, transferir, evitar ou aceitar os riscos identificados no contexto da segurança da informação.

Incidente de segurança da informação: Evento(s) de segurança da informação relacionados e identificados que podem prejudicar os ativos de uma organização ou comprometer suas operações.

Recursos de processamento de informação: Computadores, tablets, smartphones, dentre outros.

Risco: É a probabilidade de uma ameaça explorar uma vulnerabilidade e provocar um impacto.

Segurança da informação: A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações.

Vírus e software malicioso: Vírus é qualquer programa de computador que tem a capacidade de se reproduzir automaticamente, sem o conhecimento ou autorização do usuário. Em uma visão mais abrangente, software malicioso é qualquer programa de computador que realiza ações nocivas aos sistemas, como vírus, cavalo de Tróia, verme (worm) e afins.

Vulnerabilidade: Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

5. Diretrizes

5.1. Política de Segurança da Informação

A política de segurança da informação da tecnoAtiva visa garantir a satisfação dos nossos clientes e prover a melhoria contínua dos processos e serviços de tecnologia considerando: confidencialidade, integridade e disponibilidade e privacidade das informações das partes interessadas.

5.2. Do compromisso com a Segurança da Informação

A Alta Gestão da tecnoAtiva compromete-se com a implementação, manutenção e melhoria contínua da Segurança da Informação, assegurando que esta Política esteja alinhada aos objetivos estratégicos da organização, aos requisitos legais, regulatórios, contratuais e de privacidade aplicáveis, bem como às boas práticas de mercado.

Esse compromisso inclui o apoio à gestão de riscos de segurança da informação, à definição e acompanhamento de controles adequados, à conscientização dos colaboradores e terceiros aplicáveis, à proteção dos ativos de informação e à promoção de uma cultura organizacional orientada à confidencialidade, integridade, disponibilidade e privacidade das informações.

5.3. Definições Gerais

- Os ativos de informação e informações da tecnoAtiva ou sob sua custódia deverão ser utilizados exclusivamente para atender aos interesses profissionais inerentes ao negócio da empresa. A utilização destes para qualquer outro fim é proibida.

- Nenhum usuário está autorizado a revelar, divulgar ou publicar informações de propriedade ou sob custódia da tecnoAtiva, incluindo a logomarca e identidade visual da empresa, sem autorização prévia formal, independente da forma ou veículo de comunicação.

- Os ativos de informação fornecidos pela tecnoAtiva ou de terceiros que utilizem sua infraestrutura poderão ser monitorados sem aviso prévio.

- Os requisitos de continuidade, backup, restauração, redundância e recuperação devem ser definidos de acordo com a criticidade dos processos, sistemas e informações, considerando impactos ao negócio, requisitos contratuais, legais e regulatórios aplicáveis.

- O uso de inteligência artificial (IA) na organização deve ser conduzido de forma responsável, assegurando a proteção dos dados, a conformidade com leis e regulamentos. Dados sensíveis ou confidenciais só podem ser utilizados em

sistemas de IA com autorização explícita e devem estar sujeitos a controles adicionais de segurança. Conteúdo gerado por IA que seja utilizado em entregas, comunicações externas ou decisões relevantes deve passar por revisão humana antes do uso.

- O trabalho remoto na organização deve ser realizado com segurança, garantindo que todos os acessos aos sistemas e dados sejam feitos através de redes protegidas e dispositivos adequadamente configurados. Os colaboradores devem seguir as diretrizes estabelecidas para proteger as informações da empresa fora das instalações físicas, e receber treinamento adequado sobre as melhores práticas de segurança para o trabalho remoto.

5.4. Gestão de Segurança da Informação

A gestão de segurança da informação na tecnoAtiva deve ser baseada em risco e na melhoria contínua, observando requisitos contratuais, legais e regulatórios aplicáveis, bem como boas práticas de mercado, tendo como referência a ISO 27001:2022 e a ISO 27701:2019.

Controles mínimos (aplicáveis a colaboradores, terceiros e recursos tecnológicos sob responsabilidade ou custódia da tecnoAtiva):

- **Controle de acesso (senhas e MFA):** acessos devem ser individuais e intransferíveis; é proibido compartilhar credenciais; quando disponível, deve ser habilitada autenticação multifator (MFA) para acesso a e-mail, sistemas e ferramentas corporativas. Senhas devem ser mantidas em sigilo e não devem ser reutilizadas entre sistemas corporativos e pessoais.

- **Gestão de identidades:** acessos devem ser concedidos e revogados conforme necessidade de função (princípio do menor privilégio); desligamentos e mudanças de função devem resultar em revisão/revogação tempestiva de acessos; acessos privilegiados devem ser restritos e controlados.

- **Dispositivos e endpoint:** recursos de processamento de informação devem possuir proteção contra malware, atualizações aplicadas e bloqueio automático de tela; o armazenamento local de informações críticas deve ser evitado sempre que possível.

- **Classificação da Informação:** os usuários devem observar a classificação atribuída às informações e adotar os cuidados necessários para prevenir divulgação indevida, alteração não autorizada, perda, uso inadequado ou descarte inseguro.

- **Backup e restauração:** devem existir cópias de segurança para sistemas e dados relevantes, armazenadas em local seguro; testes de restauração devem ser executados periodicamente para validar a recuperabilidade.

- **Logs, monitoramento e trilhas de auditoria:** eventos de acesso e alterações em informações/sistemas críticos devem ser registrados e preservados; os registros devem permitir rastreabilidade de ações e apoiar investigação de atividades não autorizadas.

- **Gestão de vulnerabilidades e atualizações (patches):** correções de segurança devem ser aplicadas em prazo compatível com a criticidade; vulnerabilidades relevantes devem ser tratadas com prioridade e acompanhadas até a mitigação.

- **Terceiros e fornecedores:** o acesso de terceiros deve ser autorizado, limitado ao necessário e revogado ao término; requisitos de segurança e confidencialidade devem estar previstos contratualmente quando aplicável.

- **Conscientização e treinamento:** colaboradores devem realizar treinamentos de segurança conforme calendário definido pela organização e aplicar as boas práticas no dia a dia.

- **Uso aceitável:** os ativos de informação destinam-se exclusivamente a fins profissionais; a divulgação de informações, identidade visual e materiais da

empresa depende de autorização formal prévia; a organização pode monitorar ativos sob sua responsabilidade, conforme necessidade de segurança.

Devem ser priorizadas medidas preventivas ao contrário de controles reativos e, sempre que possível, as medidas de segurança devem ser atendidas através de soluções técnicas que não dependam de processos manuais ou que não estejam sujeitas a erros humanos.

O presente documento em conjunto com as Políticas e Procedimentos deve ser lido e interpretado pelos colaboradores. Qualquer dúvida relativa a esta Política deve ser encaminhada à área de TI por meio do endereço eletrônico: **servicedesk@tecnoativa.com.br.**

5.5. Revisão, Atualização e Conscientização dos Colaboradores

Esta Política deverá ser revisada no mínimo uma vez ao ano. Todos os outros documentos que derivam ou ampliam a presente Política deverão ser revisados da mesma forma.

Sempre que esta Política sofrer alterações significativas, a área de Segurança da Informação deverá avaliar a necessidade de providenciar treinamento, comunicação formal ou nova ciência aos colaboradores e áreas impactadas, de forma proporcional à relevância das alterações realizadas.

5.6. Consequências das Violações da PSI

Considera-se violação qualquer atitude que desrespeite as diretrizes estabelecidas nesta Política de Segurança da Informação ou em quaisquer das normas e documentos que a complementem. O não cumprimento desta Política de Segurança da Informação (PSI) pode ser razão para a aplicação de sanções administrativas cabíveis por parte da tecnoAtiva ao(s) colaborador(es) infrator(es). Estas sanções serão decididas pela diretoria da tecnoAtiva, podendo, ainda, ensejar advertência, suspensão ou demissão por justa causa (nos termos do art. 482, alínea "g" da CLT), sem prejuízo das possíveis consequências nas esferas cível e criminal.

Os contratos firmados pela tecnoAtiva obedecerão às penalidades previstas em caso de descumprimento das cláusulas contratuais.

5.7. Gestão de Incidentes de Segurança da Informação

Qualquer incidente ou suspeita (ex.: perda de dispositivo, acesso não autorizado, phishing, vazamento, malware, indisponibilidade relevante) deve ser reportado imediatamente à área de TI pelo e-mail **servicedesk@tecnoativa.com.br**. A tecnoAtiva deve realizar a tratativa de incidentes de acordo com o PRC.004 - Gestão de Incidentes de Segurança da Informação.

5.8. Documentos relacionados

Além desta Política, a Segurança da Informação na tecnoAtiva é regida pelas legislações e normas aplicáveis, bem como pelos seguintes documentos complementares do Sistema de Gestão:

- MAN.001 – Manual do SGI;
- PRC.004 – Gestão de Incidentes de Segurança da Informação;
- PRC.006 – Plano de Continuidade de Negócio;
- POL.003 – Política de Classificação da Informação;
- POL.005 – Política Interna;
- POL.007 - Política de Segurança da Informação para Fornecedores
- POL.008 - Política de Privacidade e Proteção de Dados.

6. Papéis e Responsabilidades

6.1. Dos usuários:

- Cumprir as diretrizes estabelecidas nesta Política de Segurança da Informação, nas normas e documentos que a complementem;

- Proteger a informação contra acesso não autorizado, divulgação, modificação, destruição ou interferência, em todo o seu ciclo de vida;

- Não ceder ou compartilhar suas credenciais de identificação, especialmente as senhas e chaves individuais de acesso aos sistemas ou à rede corporativa da tecnoAtiva para terceiros ou outros usuários;

- Realizar os treinamentos de conscientização em segurança da informação disponibilizados pela empresa;

- Reportar imediatamente à Área de Tecnologia qualquer incidente de segurança detectado, ainda que por mera suspeita;

- Sugerir medidas que possam elevar os níveis de segurança das instalações na sua área de atuação.

6.2. Da área de Tecnologia:

- Atuar de forma proativa para minimizar incidentes de segurança;

- Acompanhar a evolução tecnológica e cenário de ameaças, para definição e adoção das tecnologias e controles de segurança apropriados;

- Identificar fragilidades e exposição dos ativos de informação a ameaças significativas;

- Manter cópias de segurança dos dados de sistemas e informações da tecnoAtiva e daquelas sob sua custódia, armazenando-as em local seguro e executando testes de restauração periódica dos dados;

- Manter software antivírus devidamente instalado e atualizado em todos os computadores;

- Manter os recursos de processamento de informação da tecnoAtiva em perfeito estado para que os usuários possam executar suas atividades normalmente, sem interrupções;

- Responder imediatamente a incidentes de segurança, adotando ações emergenciais quando necessário.

6.3. Da Alta Gestão:

- Aprovar esta Política de Segurança da Informação e suas revisões, assegurando seu alinhamento aos objetivos estratégicos da tecnoAtiva;
- Apoiar a implementação, manutenção e melhoria contínua das práticas de segurança da informação;
- Disponibilizar, quando aplicável, os recursos necessários para a gestão da segurança da informação;
- Acompanhar os riscos relevantes que possam impactar a confidencialidade, integridade, disponibilidade e privacidade das informações;
- Assegurar o patrocínio necessário às iniciativas de conscientização, conformidade e governança relacionadas à segurança da informação.

7. Melhoria Contínua

A eficácia das práticas de segurança da informação deve ser acompanhada por meio de métricas, indicadores, registros, auditorias, avaliações periódicas, análise de incidentes e monitoramento dos controles aplicáveis.

Os resultados obtidos devem apoiar a identificação de oportunidades de melhoria, priorização de ações corretivas e preventivas, tratamento de riscos e aprimoramento contínuo do Sistema de Gestão.

Os planos de ação relacionados à segurança da informação devem ser acompanhados até sua conclusão, considerando prazos, responsáveis, criticidade dos riscos envolvidos e evidências de implementação, quando aplicável.

HISTÓRICO DE ALTERAÇÃO

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	22/04/2025	Wesley Ramos	Elaboração	Primeira versão
		Andrea Campelo	Aprovação	
2.0	29/04/2026	Wesley Ramos	Elaboração	Adequação referente a inclusão da ISO 27701.
		Andrea Campelo	Aprovação	
3.0	12/06/2026	Wesley Ramos	Elaboração	Detalhamento do item Documentos relacionados e ajustes gerais.
		Andrea Campelo	Aprovação	