



Política de Segurança da Informação para Fornecedores

POL.SI.03

Política do Sistema de Gestão da Arlequim

Sumário

1. Missão, Objetivos e Finalidade do Processo	2
2. Papéis e Responsabilidades do Processo (MATRIZ RACI)	2
3. Informação Documentada de Origem Interna e Externa Referenciadas	2
4. Histórico de Revisões e Aprovações	2
5. Diretrizes	2
Introdução	2
Diretrizes da Arlequim	3
Dados Pessoais	3
Conduta Ética	4
Controles e princípios	4
Aderência à Política	6

1. Missão, Objetivos e Finalidade do Processo

O propósito principal deste documento é estabelecer padrões de conduta para todos os terceiros e fornecedores em relação aos ativos de informação da Arlequim, enfatizando a conscientização sobre o uso adequado dos recursos da organização. Inclui também a definição de responsabilidades e ações disciplinares aplicáveis aos fornecedores

2. Papéis e Responsabilidades do Processo (MATRIZ RACI)

As responsabilidades relativas à execução, aprovação, consulta e informação das atividades descritas nesta política estão definidas na Matriz RACI Corporativa da Arlequim Technologies. Esse documento centraliza as responsabilidades de todos os processos organizacionais e está mantido em local controlado, sendo revisado periodicamente para garantir sua aderência às funções e estruturas da organização.

3. Informação Documentada de Origem Interna e Externa Referenciadas

Todas as informações documentadas exigidas por este procedimento ou referenciadas por este, bem como suas respectivas versões controladas, estão registradas na Lista Mestra de Documentos, conforme definido no Procedimento de Gestão da Arlequim Technologies. Documentos de origem externa que sejam aplicáveis ou necessários para o planejamento, implementação e operação do sistema de gestão também são identificados e controlados por meio da Matriz de Documentos de Origem Externa, assegurando a rastreabilidade, integridade e disponibilidade dessas informações conforme requerido pela ABNT NBR ISO/IEC 27001:2022 e ABNT NBR ISO/IEC 27701:2019.

4. Histórico de Revisões e Aprovações

Revisão	Data	Elaborador	Revisor	Aprovador	Descrição da Revisão
00	05/12/2023	Marco Rockenbach e Edson Nunes	Rafael Rabelo e Guilherme Nocera	Tiago Jesuíno	Emissão Inicial do Documento
01	01/02/2025	Marco Rockenbach e Edson Nunes	Gislaine Mereles, Carlise Amaral e Letícia Melo	Alessandra Souza	Revisão Geral da Política

5. Diretrizes

5.1 Introdução

1. Introdução: A Arlequim fundamenta-se na segurança e confidencialidade das informações ao oferecer seus serviços e produtos aos clientes. Assim, torna-se crucial que tais informações sejam salvaguardadas conforme as práticas mais eficazes, além de cumprir com exigências legais e contratuais, assegurando a confidencialidade, integridade e

acessibilidade de todos os seus ativos de informação. Este compromisso se estende também à gestão de terceiros e fornecedores, garantindo que eles também adotem medidas compatíveis para a proteção de dados e informações no âmbito de suas operações e interações com a Arlequim.

- Princípios:** Alguns princípios são adotados durante o processo de seleção e gestão de Fornecedores e Terceiros. A Arlequim enfatiza a racionalidade por meio de cautela, discernimento e juízo sólido na sua gestão e supervisão de Fornecedores e Terceiros, rejeitando comportamentos ilógicos, extravagantes e contraditórios; eficácia ao buscar a estratégia mais adequada e eficiente para atender às necessidades da Arlequim na proteção de suas informações; e neutralidade, evitando ações que causem prejuízo ou favoreçam empresas específicas.
- Responsabilidade dos Fornecedores e Terceiros:** Os fornecedores e terceiros da Arlequim são igualmente responsáveis por aderir e sustentar os fundamentos essenciais da segurança da informação:
 - Confidencialidade:** É imperativo que os Fornecedores e Terceiros ajudem na preservação da confidencialidade e na limitação do acesso a informações que são compartilhadas ou às quais têm acesso durante o desempenho de suas funções e serviços contratados. Qualquer informação partilhada ou acessível deve ser tratada como confidencial e permanece sob a propriedade da Arlequim.
 - Integridade:** Fornecedores e Terceiros devem se comprometer com a utilização correta e autorizada de ativos e informações. Está proibida qualquer alteração ou edição de informações que estejam fora do escopo de trabalho designado ou das restrições estabelecidas por procedimentos ou controles internos.
 - Disponibilidade:** Fornecedores e Terceiros devem zelar pela manutenção dos ambientes e recursos tecnológicos da Arlequim, inclusive em seus próprios fornecimentos ou suportes, com o objetivo de assegurar a continuidade dos serviços.

5.2 Diretrizes da Arlequim

- Acesso à informação:** A Arlequim adota o princípio da necessidade de conhecer (*need-to-know basis*), limitando o acesso dos fornecedores apenas às informações estritamente necessárias para o desempenho de suas funções.
 - Uso de Arlequins por Terceiros:** Visando maior segurança das informações, o Departamento de Segurança da Informação deverá analisar a necessidade de criação de um Arlequim para cada usuário vinculado a um prestador de serviço, de acordo com a criticidade das informações.
 - Uso de ferramentas Microsoft:** A Arlequim utiliza o Sistema Operacional Windows para todos os usuários corporativos, bem como produtos Office 365. Desta forma, de acordo com uma análise do departamento de segurança da informação, será optado por fornecer licenças para usuários do fornecedor ou exigir que o fornecedor utilize licenças corporativas e essas sejam vinculadas como domínio seguro.
- Monitoramento e revisão:** A Arlequim mantém rotinas de monitoramento e revisão para assegurar o cumprimento dos acordos contratuais. Isso inclui inspeções e auditorias, com intervenção quando necessário para corrigir não conformidades.
- Avaliação e Seleção de Fornecedores:** A Arlequim realiza uma avaliação minuciosa dos fornecedores potenciais para garantir que eles atendam aos padrões de segurança da informação, privacidade, qualidade e conformidade legal exigidos pela Arlequim.
- Cláusulas Contratuais:** A Arlequim incorpora cláusulas específicas nos contratos que definem os requisitos de segurança da informação, privacidade, entrega de produtos/serviços, responsabilidades legais e consequências em caso de não conformidade.

5.3 Dados Pessoais

- 1. Conformidade:** Conforme o artigo 5º da LGPD (Lei nº 13.709/2018), dados pessoais são todas as informações relacionadas a uma pessoa física identificada ou identificável, enquanto dados pessoais sensíveis referem-se a informações sobre origem racial ou étnica, crenças religiosas, opiniões políticas, filiação sindical ou a organizações de natureza religiosa, filosófica ou política, dados sobre saúde ou vida sexual, e dados genéticos ou biométricos vinculados a uma pessoa física. Além disso, a lei define controlador como a entidade (pessoa natural ou jurídica, de direito público ou privado) responsável por decisões sobre o tratamento de dados pessoais e Operador como a entidade (pessoa natural ou jurídica, de direito público ou privado) que processa dados pessoais em nome do Controlador. No contexto da Arlequim, é uma responsabilidade fundamental de todos os Fornecedores e Terceiros proteger tanto os dados pessoais quanto os dados pessoais sensíveis, seguindo as diretrizes estabelecidas pelo Controlador (neste caso, a Arlequim), quando atuarem como Operadores. Esta proteção, em conformidade com a LGPD, é uma medida de segurança crítica para assegurar a privacidade e integridade das informações dos titulares dos dados. Portanto, é crucial que todos os envolvidos obedeçam às instruções do Controlador e implementem práticas que promovam a segurança e a privacidade dos dados pessoais.

5.4 Conduta Ética

- 1. Objetivo e Alcance:** A conduta ética esperada de fornecedores e terceiros que trabalham com a Arlequim é fundamentada em princípios rigorosos de integridade, responsabilidade e respeito às normas estabelecidas. Estes princípios incluem:
 - **Integridade nas Operações:** É essencial que os fornecedores e terceiros atuem com honestidade e integridade, evitando qualquer forma de manipulação de informações, práticas antiéticas ou fraudulentas. Eles devem cumprir com todas as obrigações contratuais e legais, garantindo transparência em suas operações.
 - **Cumprimento das Leis e Normas:** Fornecedores e terceiros devem operar em total conformidade com as leis locais, nacionais e internacionais, incluindo, mas não se limitando, às normas relacionadas a trabalho, segurança, saúde e meio ambiente.
 - **Relações Transparentes e Justas:** Todas as interações e transações com a Arlequim devem ser conduzidas de maneira justa, transparente e equitativa, sem favorecimento ou discriminação.
 - **Relacionamento Colaborativo:** A Arlequim valoriza parceiros que estão dispostos a colaborar e contribuir para a melhoria contínua dos processos e produtos, promovendo uma relação de confiança e benefício mútuo.
 - **Resposta a Incidentes:** Em caso de qualquer incidente ou descumprimento das normas estabelecidas, fornecedores e terceiros devem agir prontamente para corrigir as falhas e comunicar a Arlequim, colaborando na resolução de quaisquer problemas.

5.5 Controles e princípios

- 1. Objetivo e Alcance:** Cada fornecedor deve estar ciente desta política, garantindo a confidencialidade, integridade e disponibilidade das informações, por meio da implementação e manutenção dos seguintes controles e princípios na Arlequim:
 - 1.1. Gestão de Políticas:** Garantir a confidencialidade, integridade e disponibilidade das informações por meio da definição de políticas, padrões, procedimentos e controles tecnológicos.
 - 1.2. Gestão de Riscos:** Os fornecedores devem reconhecer e informar sobre os riscos relacionados à segurança e privacidade da informação, tanto durante a aquisição quanto no controle contínuo.
 - 1.2.1.** Todos os riscos identificados pelos fornecedores devem ser gerenciados e considerados aceitáveis pela Arlequim. A preservação da confidencialidade, integridade e disponibilidade das informações é prioritária.

- 1.3. Segurança em Recursos Humanos:** Conduzir programas de conscientização e treinamento para que todos os colaboradores compreendam e se comprometam com os princípios de Segurança da Informação da Arlequim;
- 1.3.1. Assegurar a conformidade da instituição e de seus colaboradores com esta política e outras relacionadas;
 - 1.3.2. Ser responsável pelas ações dos colaboradores no uso de dispositivos tecnológicos e no acesso às informações da Arlequim, mantendo a segurança das informações durante todo o período contratual.
- 1.4. Gestão de Ativos:** Classificar as informações em categorias para proteção apropriada;
- 1.4.1. Estabelecer padrões de configuração para softwares e equipamentos utilizados pelos colaboradores.
- 1.5. Gestão de Acessos:** Proteger todas as informações da Arlequim contra acessos, modificações e destruições não autorizadas, mantendo sua confidencialidade;
- 1.5.1. Implementar um processo de gestão de acesso eficiente;
 - 1.5.2. Adotar mecanismos para garantir que o acesso às informações seja realizado apenas para finalidades autorizadas e por pessoas autorizadas;
 - 1.5.3. Assegurar que a autenticação dos usuários estejam em conformidade com os padrões da Arlequim;
 - 1.5.4. Gerir responsabilmente as credenciais de acesso dos colaboradores.
- 1.6. Segurança Física e do Ambiente:** Adotar práticas para proteção e descarte adequado das informações;
- 1.6.1. Manter segregação física em ambientes compartilhados.
 - 1.6.2. Sempre que possível é recomendado instalar barreiras físicas que exijam que os colaboradores sejam identificados por um método de identificação e autenticação (crachás de identificação, cartões eletrônicos, identificação biométrica etc.), para evitar a entrada física de pessoas não autorizadas.
 - 1.6.3. Caso sejam mantidas cópias de informações que sejam de responsabilidade da Arlequim, os sistemas onde essas informações estejam hospedadas e/ou sejam processadas deverão estar situados em uma área protegida de modo específico e que inclua, no mínimo, as seguintes medidas de segurança: i) presença de sistema de controle de acesso; ii) existência de log de entradas realizadas; iii) designação de acesso de pessoal externo apenas quando necessário e com permissão, sob supervisão contínua de pessoal autorizado.
- 1.7. Segurança nas Operações:** Implementar procedimentos e controles para prevenir intrusões e exploração de vulnerabilidades;
- 1.7.1. Gerir mudanças no ambiente produtivo de maneira segura e documentada;
 - 1.7.2. Manter um processo de backup eficaz;
 - 1.7.3. Gerir vulnerabilidades de forma proativa;
 - 1.7.4. Adotar medidas preventivas contra vazamento e violação de dados.
- 1.8. Aquisição, Desenvolvimento e Manutenção de Sistemas:** Usar sistemas fornecidos pela Arlequim apenas para as finalidades contratadas;
- 1.8.1. Adotar práticas de desenvolvimento seguro;

1.8.2. Respeitar os direitos de propriedade intelectual da Arlequim.

1.9. **Relacionamento na Cadeia de Suprimentos:** Quando o contrato permitir, garantir que subcontratados adiram às cláusulas contratuais e diretrizes da Arlequim.

1.10. **Gestão de Incidentes de Segurança da Informação:** Adotar mecanismos para prevenção de ameaças cibernéticas;

1.10.1. Direcionar incidentes cibernéticos para as equipes apropriadas da Arlequim.

1.11. **Segurança da Informação na Gestão da Continuidade dos Negócios**

1.11.1. Implementar um programa eficaz de Gestão de Continuidade de Negócios;

1.11.2. Executar testes dos planos de continuidade em casos de desastres.

1.12. **Auditoria e Gestão de Riscos:** Estar disponível para auditorias e análises de riscos, aderindo às recomendações da Arlequim.

2. **Encerramento:** Antes do término dos serviços, os fornecedores devem discutir com a Arlequim os termos e procedimentos, garantindo a segurança e privacidade da informação após o encerramento.

2.1. **Mudança ou Término de Serviços:** Qualquer alteração ou término na prestação de serviços deve ser comunicado antecipadamente à Arlequim.

2.2. **Remoção de Direitos de Acesso/Devolução de Ativos:** Ao encerrar serviços, os fornecedores devem devolver todos os ativos e remover quaisquer direitos de acesso, garantindo a confidencialidade das informações.

5.6 Aderência à Política

1. **Não aderência:** Em caso de não aderência ou descumprimento desta política, a Arlequim adotará medidas necessárias para corrigir a situação.

2. **Alto padrão:** Esses protocolos asseguram que os fornecedores e terceiros da Arlequim mantenham um alto padrão de segurança e ética nas suas operações e no manuseio das informações.