POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Controle de alterações

Revisão	Data	Local da Revisão	Descrição
0	17/06/2019		Emissão inicial
1	11/04/2022	Itens 2, 3 e 4	Item 2: Inclusão da definição do Comitê Executivo de Segurança; Item 3: Atribuições do Comitê Executivo de Segurança; Item 4: Inclusão da Declaração de Comprometimento da Direção; inserção de algumas diretrizes no item de Cuidados com a Informação; alteração do e-mail de resposta a incidentes e pequenos ajustes de redação.

Lista de Distribuição

Função
Todos os administradores e colaboradores do Magazine Luiza e empresas coligadas.

Lista de Treinamento

Função
Todos os administradores e colaboradores do Magazine Luiza e empresas coligadas.

Elaborado/Revisado por:

Diretoria de Segurança da Informação
Diretoria de Compliance, Integridade e PLD
Diretoria Jurídica

Aprovado por:

Conselho de Administração, em 19/04/2022

1. OBJETIVO

Definir os requisitos para estabelecer, implantar, manter e melhorar continuamente um sistema de gestão da segurança da informação no Magazine Luiza e suas empresas coligadas ("Grupo Magalu"). Além disso, determinar a infraestrutura tecnológica necessária para assegurar a confidencialidade, integridade e disponibilidade das informações do Magazine Luiza junto a agentes e entes autorizados, **em conformidade com as exigências, para o segmento, estabelecidas na Lei Federal nº 13.709 de 14 de Agosto de 2018.**

2. TERMOS E DEFINIÇÕES

- **Ativos Tecnológicos:** No contexto de Segurança da Informação, é qualquer bem ou direito que tenha valor para a Empresa, como computadores, dispositivos móveis, sistemas, aplicativos, bases de dados, informações, sala de servidores, entre outros.
- **Colaboradores:** São todos que têm ou tiveram algum vínculo com o Magazine Luiza, assim compreendido: empregados, ex-empregados, aprendizes, ex-aprendizes, estagiários, ex-estagiários, prestadores de serviço, ex-prestadores de serviços, diretores, sócios, terceiros, parceiros ou ex-parceiros, visitantes que têm, terão ou tiveram acesso às informações da Empresa e/ou utilizam, utilizarão ou utilizaram sua infraestrutura tecnológica, mesmo após o término do regime jurídico a que estavam submetidos.
- **Comitê Executivo de Segurança (CES):** Formado pelas Diretorias Executivas de: (i) Administração e Controle, (ii) da Diretoria (s) Executiva (s) responsável (is) pela (s) área (s) impactada pelo incidente (iii) Diretoria Executiva Responsável pelo Relacionamento com Investidores; e, pelos Vice-Presidente de Plataforma e de Negócios. O Comitê será secretariado pela Diretoria de Compliance, Integridade e PLD. As deliberações serão subsidiadas pelos dados e apurações realizadas pela Diretoria de Segurança da Informação e/ou da Gerência de Privacidade, para os casos de incidentes de privacidade.
- **Comitê Operacional de Segurança (COS):** Formado pelas Diretorias de Áreas Funcionais de: (i) Segurança da Informação, (ii) Jurídica, (iii) Auditoria Corporativa, (iv) *Compliance*, Integridade e PLD, e pela Gerência de Reputação e Sustentabilidade.
- **Dados Pessoais**: Informações que identificam indivíduos como, por exemplo: CPF, Nome Completo, RG, email, telefone celular, entre outros.
- **Dados Pessoais Sensíveis**: Informações sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

- **Grupo Magazine Luiza (Magalu)**: Significa o Magazine Luiza S.A., suas subsidiárias integrais e empresas controladas, direta ou indiretamente, e empresas coligadas. A depender do contexto, pode incluir também outros parceiros, como sellers, anunciantes do parceiro Magalu e outros.
- **Segurança da Informação:** Preservação da confidencialidade, integridade e disponibilidade de dados e informações pertencentes ao Grupo Magalu. Adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, também poderão estar envolvidos. Visa proteger a informação de ameaças para garantir a continuidade dos negócios, minimizar os danos, maximizar o retorno dos investimentos e de novas oportunidades de transação.
- **Sistema da Informação**: Um conjunto organizado de elementos, podendo ser pessoas, dados, atividades ou recursos materiais em geral. Estes elementos interagem entre si para processar informação e divulgá-la de forma adequada em função dos objetivos de uma organização.

3. ATRIBUIÇÕES E RESPONSABILIDADES

Cargos/Diretoria	Responsável por
Conselho de Administração	• Avaliar e aprovar a Política de Segurança da Informação e suas demais Políticas, em conformidade com a sua alçada; • Conhecer e exigir a implantação e a aplicação das Políticas de Segurança da Informação.
Presidência Executiva e Vice Presidente de Plataforma	• Assegurar que a Política de Segurança da Informação e os objetivos de segurança da informação estão estabelecidos e são compatíveis com a direção estratégica da organização; • Assegurar que os recursos necessários para o sistema de gestão da segurança da informação estão disponíveis; • Promover a cultura de segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação.

Diretoria Executiva e Diretoria de Áreas Funcionais	• Conhecer e assegurar que todos os colaboradores de suas respectivas áreas sejam treinados quanto ao tema, quando necessário; • Observar todas as diretrizes desta política que são aplicáveis à sua área, e garantir que sejam aplicadas por todos os seus liderados; • Comunicar a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do sistema de gestão da segurança da informação.
Comitê Executivo de Segurança	• Garantir a aplicabilidade desta política; • Trabalhar para que todos os recursos necessários à aplicação da presente política sejam disponibilizados; • Analisar a documentação de segurança da informação com o intuito de verificar se a mesma é aplicável ao Magazine Luiza, de acordo com o negócio da empresa; • Autorizar as exceções da presente política; • Reportar ao Conselho de Administração eventuais fragilidades ou falhas graves; • Monitorar periodicamente a efetividade da aplicação da presente política por meio de reporte das áreas operacionais e, ainda, quando possível, pela execução de Avaliações de Controles de Segurança da Informação.
Comitê Operacional de Segurança	• Analisar os impactos operacionais decorrentes da aplicação das normas de Segurança da Informação; • Checar a eficácia e efetividade dos mecanismos e instrumentos instituídos/implantados, pelo Magazine Luiza, para garantir a segurança da informação; • Definir retenção para guarda de logs e conversas telemáticas e telefônicas; • Tratar as externalidades negativas oriundas de ocorrência de segurança da informação; • Reportar ao Comitê Executivo de Segurança da Informação eventuais fragilidades ou riscos que possam gerar perdas financeiras, impacto a reputação ou aplicação de sanções; • Requisitar a revisão desta política sempre que identificar necessidades de adequações.

Diretoria Jurídica	• Monitorar e notificar o Conselho de Administração quanto a existência, criação e atualização de legislações vigentes e aplicáveis ao Magazine Luiza e suas empresas coligadas referentes aos temas de Privacidade e Segurança da Informação; • Garantir que terceirizados e fornecedores que manipulam dados originados no Magazine Luiza e suas empresas coligadas assinem os termos de confidencialidade e o aditivo de Segurança da informação.
Diretoria de Segurança da Informação	• Elaborar e instituir, com o apoio da área de Compliance, Integridade e PLD, sempre que necessário, novas políticas de Segurança da Informação; • Instituir, sempre que necessário e/ou demandado pelo Comitê Executivo de Segurança, instrumentos de controle de violações às diretrizes aqui estabelecidas; • Treinar, com o apoio da área de gestão de pessoas, todos os colaboradores e conscientizá-los acerca das diretrizes e regulamentos da Segurança da Informação; • Revisar, sempre que necessário e/ou demandado pelo Comitê Executivo de Segurança a presente política e outras normas de Segurança da Informação e/ou relacionadas; • Reportar ao Comitê Executivo de Segurança qualquer tipo de incidente e/ou violações relacionadas a presente política e incidentes de SI que possam gerar riscos financeiros, reputacionais, regulatórios ou judiciais; • Propor e, quando necessário, conduzir a execução de ações corretivas ou preventivas pertinentes a qualquer matéria relacionada à segurança da informação; • Monitorar a efetividade e a eficácia da aplicação dos instrumentos e/ mecanismos de controle instituídos e de todos os requisitos estabelecidos pela presente política.
Diretoria de Dados	• Aplicar os controles definidos pela Diretoria de Segurança da Informação; • Assegurar a governança dos dados com confidencialidade, disponibilidade e integridade; • Aplicar o princípio do privilégio mínimo de acesso nas áreas solicitantes baseados somente na necessidade,

	considerando anonimização de dados sensíveis.
Diretoria Compliance, Integridade e PLD	• Subsidiar a avaliação do Comitê Executivo de Segurança da Informação, disponibilizando as informações e os dados necessários para execução de suas atribuições; • Apoiar a diretoria de Segurança da Informação na elaboração de políticas e procedimentos e na adoção e institucionalização de mecanismos e instrumentos de controle relacionados aos requisitos estabelecidos na presente política; • Auxiliar a Diretoria de Segurança da Informação na divulgação e nos treinamentos acerca dos requisitos de segurança da informação; • Auxiliar na elaboração de plano de ações corretivas e preventivas; • Sugerir adequações legais das políticas, controles e procedimentos; • Conduzir processos de verificação de Compliance, com a finalidade de checar a eficácia e efetividade dos requisitos estabelecidos na presente política.
Auditoria Corporativa	• Auditar os processos, procedimentos e mecanismos de segurança da informação, apontando, quando identificado/necessário, não conformidades, oportunidades de melhorias; • Auditar, periodicamente ou sempre que houver necessidade, os ativos tecnológicos e da informação e sua utilização.
Gestão de Pessoas	• Informar as diretrizes presentes nesta política aos novos colaboradores, • Apoiar a Diretoria de Segurança da Informação no treinamento de todos os colaboradores e na conscientização acerca das diretrizes e regulamentos de Segurança da Informação; • Assegurar que todos os ativos fornecidos aos colaboradores, durante a vigência de seu contrato, sejam devolvidos, no momento em que ocorrer a extinção do vínculo; • Informar às áreas responsáveis acerca da remoção de acessos físicos ou acessos lógicos aos sistemas de informação, no momento em que ocorrer o desligamento

	do colaborador ou o encerramento do contrato de prestação de serviço e as alterações de cargo/área. ● Disponibilizar os documentos relacionados à Segurança da Informação aos colaboradores, além de custodiar e colher assinatura do "Termo de Ciência e Responsabilidade" na admissão de novos colaboradores.
Gerências e Demais lideranças	● Fazer e garantir que seus liderados façam todos os treinamentos necessários, com o intuito de assegurar que as medidas de segurança da informação referentes à sua área estão sendo observadas; ● Avaliar periodicamente os privilégios atribuídos a cada Perfil de Acesso; ● Assegurar que todos os ativos fornecidos aos colaboradores, durante a vigência de seu contrato, sejam devolvidos no momento em que ocorrer a extinção do vínculo; ● Informar às áreas responsáveis acerca da remoção de acessos físicos ou acessos lógicos aos sistemas de informação no momento em que ocorrer o desligamento do colaborador ou o encerramento do contrato de prestação de serviço, ou adequação de perfis nas alterações de cargo/área.
Responsável pela Informação	● Classificar e garantir que os controles necessários para a confidencialidade, integridade e disponibilidade da informação estão sendo aplicados; ● Mapear as funcionalidades críticas dos sistemas e definir Perfis de Acesso, considerando a relevância das transações.
Responsável pelo Sistema da Informação	● Requisitar que todos os controles de Segurança da Informação foram desenvolvidos, adquiridos e implantados; ● Garantir que todos os controles de Segurança da Informação foram devidamente aprovados pela Diretoria de Segurança da informação; ● Requisitar que os ativos possuam proteção contra Códigos Maliciosos, bem como que recebam as atualizações necessárias; ● Assegurar que os acessos nos sistemas de informação sejam feitos mediante identificação única, pessoal e

	intransferível; ● Realizar o descarte de informações confidenciais por meio de recursos que resultem na descaracterização do seu conteúdo.
Colaboradores	● Respeitar as diretrizes de Segurança da Informação estabelecidas nas políticas; ● Fazer todos os treinamentos indicados para o exercício de sua função, e, sempre que sentir necessidade, procurar ajuda/esclarecimentos com a área de Segurança da Informação; ● Notificar à Diretoria de Segurança da Informação ou Compliance, Integridade e PLD sempre que identificar uma violação das diretrizes citadas nesta política; ● Notificar à Diretoria de Segurança da Informação caso identifique a existência de fragilidades ou eventos de falha na Segurança da Informação; ● Sugerir melhorias de controles, políticas e procedimentos, em seus processos, quando necessário.

4. DIRETRIZES PARA SEGURANÇA DA INFORMAÇÃO

Toda e qualquer informação gerada, obtida, adquirida ou processada pelo Grupo Magalu, é considerada de sua propriedade, devendo ser utilizada exclusivamente para seus interesses.

A informação é um ativo de extremo valor e importância, sendo esse um elemento fundamental para a estratégia de negócio da empresa. Portanto, no uso, disponibilização e/ou compartilhamento das informações do Grupo Magalu, todos os colaboradores, parceiros, terceiros, administradores e acionistas devem respeitar os requisitos definidos nesta Política e nas outras políticas, procedimentos e manuais relacionados.

Em linhas gerais, as informações e dados da empresa não devem ser divulgados, mesmo que internamente, para pessoas não autorizadas. A divulgação em ambiente externo exige prévia autorização, conforme critérios definidos na Política de Tratamento da Informação, que se encontra em conformidade com a matriz de alçadas do Grupo Magalu.

Com a finalidade de assegurar a observância dessas diretrizes são adotadas medidas de segurança que evitam o compartilhamento indevido de informações sensíveis da empresa, bem como o uso inadequado da nossa infraestrutura.

O Grupo Magalu trabalha para que todos os seus colaboradores, parceiros, terceiros,

administradores e acionistas respeitem e assegurem a confidencialidade, integridade e disponibilidade de dados e/ou informações a que tiverem acesso e/ou fizerem uso.

4.1. Declaração de Comprometimento da Direção

A diretoria do Grupo Magalu está comprometida e apoia as metas e princípios de Segurança da Informação e Privacidade na proteção de seus ativos tangíveis e intangíveis de acordo com as necessidades de negócio e em conformidade legal, garantindo a sua confidencialidade, integridade, disponibilidade, autenticidade e legalidade.

4.2. Diretrizes de Cuidados com a Informação

- O acesso às informações classificadas como confidencial, uso restrito e uso interno para o Grupo Magalu, deverá ser restrito e controlado, nos termos da Política de Classificação de Informação. Neste sentido, deverão ser implantados controles para garantir que as informações sejam conhecidas, alteradas e acessadas somente por pessoas autorizadas;
- Os ativos relacionados com a geração, armazenamento e processamento de informações deverão ser controlados e inventariados;
- A utilização dos ativos deverá ser previamente autorizada, e seu uso restrito às atribuições necessárias para que os Colaboradores exerçam suas atividades;
- O Responsável pela Informação deve implantar todos os controles necessários para a devida proteção da Informação de acordo com a classificação da informação;
- O colaborador é totalmente responsável pela custódia de suas senhas de acesso à rede, sistemas, e-mails, entre outros, de tal modo que é responsável por todos os atos executados com seu login;
- Toda informação recebida, gerada, armazenada, processada, transmitida e descartada em decorrência das operações do Grupo Magalu são de propriedade da organização. É vedado o armazenamento, a cópia, o uso e a transmissão de informações para pessoas não autorizadas.

4.3. Diretrizes de Treinamento e Conscientização

- Os colaboradores, antes de assumir suas funções devem realizar o treinamento de Segurança da Informação e treinamento adequado para suas funções;
- Todos os colaboradores devem realizar treinamento de reciclagem de Segurança da Informação dentro de um período de 12 meses da sua contratação;
- Campanhas de Segurança da Informação devem ser efetuadas periodicamente a fim de manter a importância e conscientização sobre o tema.

4.4. Diretrizes de Violações e Incidentes de SI

- É responsabilidade de todo colaborador informar a Diretoria de Segurança da Informação qualquer ação que possa violar a confidencialidade, integridade e disponibilidade das informações do Grupo Magalu através do email: csirt@magazineluiza.com.br;
- A Diretoria de Segurança da Informação deverá investigar qualquer suspeita de violação de SI assim como reportar os resultados para o Comitê Executivo de Segurança da Informação;
- Sob suspeita de qualquer violação, a Diretoria de Segurança da Informação poderá retirar o equipamento em posse dos colaboradores sem aviso prévio para realizar a investigação.

4.5 Diretrizes de Gestão de Riscos de SI

- É responsabilidade da Diretoria de Segurança da Informação avaliar riscos inerentes a Segurança da Informação nos ativos de TI do Grupo Magalu;
- Todo desenvolvimento, aquisição, implantação e grandes mudanças de sistemas no Grupo Magalu deve ter uma avaliação formal de riscos de SI assim como o direcionamento de requisitos pela Diretoria de Segurança da Informação antes de utilizar dados produtivos e sensíveis de acordo com a Política de Classificação da Informação;
- Seguir as diretrizes descritas na Política de Gestão de Riscos de Segurança da Informação.

5. DISPOSIÇÕES GERAIS

5.1. Aplicabilidade

Esta Política se aplica, irrestritamente, a todos os administradores, colaboradores, parceiros, fornecedores e empresas coligadas do Magazine Luiza.

5.2. Exceções

Todas as exceções às diretrizes das políticas de segurança da informação devem ser analisadas pelo Comitê Executivo de Segurança da Informação e os riscos devidamente tratados conforme a Política de Gestão de Riscos de Segurança da Informação.

Nota 1: O conjunto de diretrizes acima não se esgotam nesta Política e nos regulamentos específicos. Em razão da constante evolução tecnológica, é obrigação do colaborador adotar todo e qualquer outro procedimento de segurança, homologado pela equipe de

segurança da informação, que esteja ao seu alcance, visando proteger todas as informações do Magazine Luiza.

5.3. Vigência e Aprovação

Esta Política tem vigência a partir da data de sua aprovação pelo Conselho de Administração podendo ser revisada sempre que necessário.

5.4. Criação do Comitê Executivo e o Operacional de Segurança da Informação

Fica instituído, por meio desta Política, o Comitê Executivo de Segurança da Informação e o Comitê Operacional de Segurança da Informação.

5.5. Política de Consequências a Violações

Qualquer violação à presente política será passível de penalização de acordo com a gravidade da falta cometida, que poderá ser desde advertência e suspensões disciplinares até demissão por justa causa ou rescisão contratual.

Os colaboradores, ainda, enquanto vigorar o regime jurídico o qual estiverem submetidos, ou, após a eventual rescisão, estão sujeitos a todas e quaisquer medidas judiciais em razão do ato ilícito praticado, como indenização por perda e danos, além da aplicação dos procedimentos criminais pertinentes, tais como crimes relacionados à concorrência desleal, divulgação de informações sensíveis, entre outros existentes no Código Penal Brasileiro e demais legislações aplicáveis.

As medidas de consequências adotadas pelo Magazine Luiza, seja no âmbito interno, ou por meio de adoção de medida judicial cabível, serão aplicadas após a avaliação da gravidade do caso concreto e dos impactos causados pela violação.

Compete à Auditoria Corporativa, em conjunto com a Diretoria de Segurança da Informação conduzir os processos de apuração dos incidentes relatados e submetê-los ao Comitê Executivo de Segurança, que, em casos graves, ratificarão a decisão com o Conselho de Administração.

As sanções à presente política serão aplicadas pelo Comitê Disciplinar , em conformidade com a Política de Consequências.

6. REFERÊNCIA

- Código de Ética e Conduta;
- Política de Classificação da Informação;

- Política de Gestão de Riscos de Segurança da Informação;
- NBR ISO/IEC 27001:2013, Sistemas de Gestão de Segurança da Informação;
- NBR ISO/IEC 27002:2013, Código de prática para a gestão da Segurança da Informação;
- Lei Federal nº. 9.279/1996, que regula direitos e obrigações relativos à propriedade intelectual;
- Lei Federal nº 9.609/1998, que dispõe sobre a proteção da propriedade intelectual de programa de computador;
- Lei Federal nº 9610/1998, que altera, atualiza e consolida a legislação sobre direitos autorais;
- Lei Federal nº 12.965/2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;
- Lei Federal nº 13.709/2018, dispõe sobre a proteção de dados pessoais.