

Junho de 2023

Título	Política de Segurança da Informação
Número de referência	002
Número de versão	V 03
Status	Aprovada
Aprovador	CEO
Data da aprovação	14/06/2023
Data da próxima revisão	14/06/2024
Área responsável	Gerência de Riscos e <i>Compliance</i>
Normas externas edocumentos relacionados	Lei 13.709/2018 e Resolução CMN 4.658/2018
Normas internas relacionadas	Política de Risco Operacional e de Segurança Cibernética

REVISÃO		ÁREA RESPONSÁVEL	APROVADOR	DESCRIÇÃO DA ALTERAÇÃO
Versão	DATA			
01	04/02/2021	Área de Riscos	CEO e VP	Implementação
02	25/02/2022	Área de Riscos	CEO	Revisão periódica
03	01/02/2022	Área de Riscos	CEO	Atualização da razão social
04	14/06/2023	Área de Riscos	CEO	Atualização de revisão de política

Sumário

1	Objetivo	2
2	Abrangência	2
3	Base Legal	2
4	Diretrizes	2
5	Processo de Segurança da Informação.....	4
6	Classificação da Informação.....	4
7	Glossário	5

1 Objetivo

Esta política orienta a Holding e suas empresas na gestão da segurança da informação, demonstrando o compromisso com a proteção das informações corporativas e demais ativos de informação.

2 Abrangência

Todos os administradores (Diretoria e demais gestores) e colaboradores das empresas ligadas e controladas pela Valloo (Valloo Tecnologia, Valloo Benefícios, Valloo Digital e Valloo Instituição de Pagamento) doravante denominadas “Valloo S.A.” ou “Holding”.

3 Base Legal

A Valloo se utiliza dos padrões ISO 27001 e 27002:2013 que tratam de sistemas de gestão da segurança da informação e os requerimentos da Lei Geral de Proteção de Dados - LGPD nº. 13.709/2018, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade.

4 Diretrizes

4.1 Consideramos, na formulação desta Política, as demais diretrizes estabelecidas nos demais documentos corporativos da Valloo;

4.2 Tratamos a informação, na gestão empresarial, como ativo e alinhamos a gestão da segurança da informação aos nossos negócios;

- 4.3 Planejamos, dimensionamos e orientamos a proteção dos ativos de informação para atender aos interesses estratégicos da Holding;
- 4.4 Garantimos a confidencialidade, integridade, disponibilidade, legalidade, rastreabilidade e autenticidade da informação em todo o seu ciclo de vida (produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte), de modo ético e responsável;
- 4.5 Protegemos e monitoramos os ativos de informação reduzindo a possibilidade de uma descontinuidade operacional em caso de incidentes de segurança da informação;
- 4.6 Classificamos a informação em relação ao seu valor ou criticidade para a Holding;
- 4.7 Identificamos e corrigimos as vulnerabilidades, as ameaças, os riscos e os impactos nocivos que envolvam os ativos de informação da Companhia, por meio de procedimentos de teste e de avaliação periódicos, a intervalos regulares;
- 4.8 Aplicamos proteção aos ativos de informação de forma compatível com sua criticidade e impacto aos resultados, nas nossas atividades e na reputação da Holding, alcançando todos os processos, informatizados ou não;
- 4.9 Adotamos mecanismos de proteção contra uso indevido, fraudes, danos, perdas, erros, sabotagens e roubo, quando do tratamento (produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte) das informações geradas ou utilizadas pelo Grupo;
- 4.10 Analisamos as ocorrências de tratamento indevido de informações corporativas, sob os aspectos legal e disciplinar, imputando responsabilização e, sob o aspecto técnico, corrigindo as vulnerabilidades;
- 4.11 Procedemos à identificação e definição de, pelo menos, um gestor da informação e atribuímos-lhe responsabilidades sobre a informação em todo o seu ciclo de vida;
- 4.12 Identificamos, nos sistemas de controle de acesso, cada usuário individualmente, responsabilizando-o, juntamente com o administrador que lhe concedeu o acesso, pelo tratamento indevido das informações corporativas, realizado sob seu código de identificação;
- 4.13 Obedecemos ao princípio de segregação das funções de desenvolvimento de recursos, uso de recursos, administração da segurança e auditoria, na gestão da informação;
- 4.14 Disponibilizamos para os usuários as informações da Valloo e de suas empresas com o objetivo de viabilizar suas atividades profissionais na Companhia. Não permitimos a utilização das informações para qualquer atividade que viole esta Política;
- 4.15 Preservamos nossos requisitos de segurança da informação, na contratação de serviços ou de pessoas e no relacionamento com colaboradores, fornecedores, terceiros, parceiros, contratados e estagiários;

4.16 Disseminamos questões sobre segurança da informação por meio de programas permanentes de conscientização, de abrangência geral, ou cursos de capacitação técnica para os usuários diretamente envolvidos na utilização de recursos;

4.17 Identificamos, analisamos, avaliamos e tratamos os riscos que envolvam os ativos de informação, por meio de avaliações periódicas, a intervalos regulares;

4.18 Concedemos a funcionários e a terceiros somente o acesso às informações necessárias ao desempenho de suas funções e atribuições previstas em contrato ou por determinação legal.

5 Processo de Segurança da Informação

Os controles a seguir fornecem a base do processo de Segurança da Informação na Valloo, estabelecem as regras para proteger as informações e estão amparados nos seguintes pilares de governança e melhores práticas:

5.1 Garantia da segurança e a confidencialidade das informações de clientes, parceiros, fornecedores e empregados;

5.2 Proteção contra ameaças ou riscos à segurança dessas informações;

5.3 Proibição do acesso não autorizado ou o uso de informações que possam prejudicar os clientes ou empregados;

5.4 Armazenamento, transporte e descarte adequado de informações de clientes, parceiros, fornecedores e empregados;

5.5 Informação aos empregados sobre suas responsabilidades de proteger as informações sob custódia da Valloo e a segurança dos sistemas;

5.6 Garantia de que os prestadores de serviços terceirizados relevantes cumpram nossas políticas e normas de segurança, bem como as obrigações regulamentares aplicáveis;

5.7 Cumprimento de todos os requisitos de notificação do cliente para proteção das informações.

6 Classificação da Informação

A classificação define o nível de sensibilidade da informação a fim de assegurar que receba o nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a Valloo, e são assim tratadas:

6.1.1 Informação Pública (#pública) - A informação recebe essa classificação quando puder ser divulgada a todos (funcionários, terceirizados, clientes, fornecedores e público em geral), sem que isso provoque impactos no negócio. Apesar de não precisar de nenhum tipo de proteção quanto à questão do sigilo, é conveniente que somente o usuário que precise de tal informação para o desempenho de suas atividades tenha acesso a ela;

6.1.2 Informação Interna (#interna) - A informação é assim classificada quando deve ser conhecida somente por pessoas de dentro da Holding. Contudo, caso haja vazamento e ela se torne de conhecimento público, é característica desse tipo de informação a impossibilidade da ocorrência de prejuízos ao Grupo. Como são informações relevantes para o funcionamento dos negócios, precisam principalmente ter sua integridade protegida;

6.1.3 Informação Confidencial (#confidencial) - A informação deve ser assim classificada quando acessos não autorizados a ela, mesmo que por membros da própria organização, sejam capazes de trazer sérios danos ao negócio. Logo, a informação confidencial precisa ser protegida contra acessos internos e externos e receber o grau de proteção mais elevado. Só devem ter acesso a informações confidenciais pessoas que necessitem dessas informações para a realização de suas atividades, independentemente do cargo ocupado.

6.2 Cada colaborador é responsável, juntamente com seu gestor, pela classificação da informação por ele produzida e aplicação das cautelas definidas, tais como a adequada guarda, acesso, tratamento e destruição da informação.

7 Glossário

Para fins desta Política são considerados os seguintes conceitos:

7.1 Administrador de Acesso: aquele que gerencia o direito de acesso às informações em meio eletrônico;

7.2 Anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

7.3 Ativo de Informação: base de dados e arquivos, contratos e acordos, documentação de sistema, informações sobre pesquisa, manuais de usuário, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas;

7.4 Ciclo de vida da informação: compreende as fases de vida da informação, que são: produção, manuseio, reprodução, transporte, transmissão, armazenamento e descarte;

7.5 Classificação da Informação: identificar quais são os níveis de proteção que as informações demandam, se públicas, internas, confidenciais ou restritas;

7.6 Confidencialidade: propriedade que garante que a informação está disponível ou revelada a usuário autorizado;

7.7 Consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda como tratamento de seus dados pessoais para uma finalidade determinada;

7.8 Disponibilidade: propriedade de ser acessível e utilizável por um usuário autorizado;

7.9 Dado Pessoal: informação relacionada a pessoa natural identificada ou identificável;

7.10 **Dado Pessoal Sensível:** dado pessoal 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;

7.11 **Eliminação:** exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado;

7.12 **Gestor da Informação:** área responsável pela gestão da informação (em suas diversas formas), durante todo o seu ciclo de vida, dentro do escopo de suas atribuições e/ou responsabilidades;

7.13 **Incidentes de Segurança da Informação:** qualquer ação que possa causar a quebra de confidencialidade, integridade e/ou disponibilidade das informações da Companhia;

7.14 **Informação:** dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

7.15 **Integridade:** salvaguarda da exatidão e completeza da informação e dos métodos de processamento de forma que as alterações sejam planejadas e autorizadas;

7.16 **Princípio de Segregação das Funções:** consiste na separação de atribuições ou responsabilidades entre diferentes pessoas, especialmente as funções ou atividades chave de autorização, execução, aprovação, registro e revisão ou auditoria;

7.17 **Segurança da Informação:** preservação da confidencialidade, integridade e disponibilidade das informações;

7.18 **Terceiros:** pessoas físicas, que não são empregados da Companhia, e pessoas jurídicas, que estabeleçam relacionamento com a Companhia por interesse do serviço, previsão contratual ou imposição legal;

7.19 **Titular:** pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

7.20 **Tratamento:** toda operação realizada com dados, tais como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

7.21 **Usuário:** aquele que tem acesso à informação corporativa.

02_Política de Segurança da Informação.pdf

Documento número #a0b589a5-8db6-4c1a-87a3-5b76ede3b467

Hash do documento original (SHA256): 406a75560f78c79ae6ada478d447ffcd970d4ff2e6d496d468979f6c6ba9392c

Assinaturas



José Luiz Araújo

CPF: 305.389.711-34

Assinou para aprovar em 15 jun 2023 às 21:56:41

Log

- 15 jun 2023, 14:39:59 Operador com email rafael.vilela@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae criou este documento número a0b589a5-8db6-4c1a-87a3-5b76ede3b467. Data limite para assinatura do documento: 21 de julho de 2023 (14:32). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
- 15 jun 2023, 14:40:02 Operador com email rafael.vilela@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae adicionou à Lista de Assinatura: ze@valloo.com.br para assinar para aprovar, via E-mail, com os pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP.
- 15 jun 2023, 21:56:41 José Luiz Araújo assinou para aprovar. Pontos de autenticação: Token via E-mail ze@valloo.com.br. CPF informado: 305.389.711-34. IP: 172.226.128.1. Componente de assinatura versão 1.516.0 disponibilizado em <https://app.clicksign.com>.
- 15 jun 2023, 21:56:42 Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número a0b589a5-8db6-4c1a-87a3-5b76ede3b467.



Documento assinado com validade jurídica.

Para conferir a validade, acesse <https://validador.clicksign.com> e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.

As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº a0b589a5-8db6-4c1a-87a3-5b76ede3b467, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.