Abril de 2025

Título	Política de Segurança Cibernética
Número de referência	006
Número de versão	V 06
Status	Aprovada
Aprovador	Diretora Presidente
Data da aprovação	22/04/2025
Data da próxima revisão	22/04/2026
Área responsável	Diretoria Executiva de Infra e Segurança
Normas externas e documentos relacionados	Resolução CMN 4.893/2021
Normas internas relacionadas	Política e procedimentos do PCI-DSS

REVISÃO		**ÁREA RESPONSÁVEL**	**APROVADOR**	**DESCRIÇÃO DA ALTERAÇÃO**
Versão	**DATA**			
01	04/12/2020	Área de Riscos	CEO e VP	Implementação
02	25/02/2022	Área de Riscos	CEO	Revisão periódica
03	01/02/2023	Área de Riscos	CEO	Atualização da razão social
04	27/12/2024	Diretoria Executiva de Governança, Risco e Compliance	Diretora Presidente	Assinatura da Diretora Presidente
05	22/04/2025	Diretoria Executiva de Infra e Segurança da Informação	Diretora Presidente	Revisão periódica

Sumário

1. Objetivo

O objetivo desta política é estabelecer diretrizes e responsabilidades para o gerenciamento da segurança cibernética garantindo a integridade, confidencialidade e disponibilidade de informações e para a promoção da melhoria contínua nos procedimentos e controles relacionados a ela. Essa política apresenta os requisitos mínimos para a contratação de serviços de processamento e armazenamento de dados na nuvem, em cumprimento aos requisitos legais vigentes e deve ser seguida por todos os colaboradores e prestadores de serviços com acesso a qualquer tipo de dado sob a responsabilidade da Valloo.

2. Abrangência

A Segurança Cibernética e a presente Política aplicam-se a todos os gestores e colaboradores da Valloo, empresas ligadas e controladas pela Valloo e empresas contratadas pela Valloo para prestação de serviços.

Cabe à Diretoria Executiva de Infraestrutura e Segurança da Informação a responsabilidade pela gestão da Segurança Cibernética e atualizações da presente Política.

3. Base Legal

A Valloo segue os requerimentos da Resolução CMN 4.893/2021 (com correção de redação dada a partir de 01/3/24 pela Resolução CMN 5.117/2024) que dispõe sobre a política de segurança cibernética e os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil.

4. Procedimentos e Controles para Segurança Cibernética

A fim de reduzir a vulnerabilidade à incidentes de segurança e cumprir os objetivos da segurança cibernética, a àrea de Segurança da Informação da Valloo é responsável pela criação, proposição, administração e supervisão de políticas e procedimentos concebidos para garantir que os riscos sejam identificados e gerenciados dentro de tolerâncias corporativas definidas, incluindo a prevenção, detecção, contenção e correção de violações de segurança cibernética.

i. Os programas são documentados e atualizados anualmente para garantir a conformidade contínua com os requisitos regulamentares e são baseados nas melhores práticas reconhecidas pelo mercado tais como:Garantir a segurança e a confidencialidade das informações de clientes, parceiros, fornecedores e empregados.

ii. Proteger contra ameaças ou riscos à segurança dessas informações.

iii. Proibir o acesso não autorizado ou o uso de informações que possam prejudicar os clientes ou empregados.

iv. Armazenar, transportar e descartar adequadamente informações de clientes, parceiros, fornecedores e empregados.

v. Informar os empregados sobre suas responsabilidades de proteger as informações sob custódia da Valloo e a segurança dos sistemas.

vi. Garantir que os prestadores de serviços terceirizados relevantes cumpram nossas políticas e normas de segurança, bem como as obrigações regulamentares aplicáveis.

vii. Cumprir todos os requisitos de notificação do cliente para proteção das informações.

5. Políticas que formam os Pilares da Segurança Cibernética

Para abranger os procedimentos e controles que assegurem a integridade, confidencialidade e disponibilidade de informações que formam os pilares da Segurança Cibernética, a área de Segurança da Informação da Valloo publicou as seguintes políticas que devem ser compreendidas como complementares à esse documento:

i. Política de Gestão de Acessos – institui procedimentos para concessão de acessos e bloqueios aos sistemas, visando a preservação de informações críticas ou sigilosas, o acesso aos sistemas e equipamentos.

ii. Política de Gestão de Ativos – institui procedimentos para a utilização, manutenção e gestão de ativos da Valloo, visando proteger a integridade e confidencialidade do negócio.

iii. Plano de Respostas aos Incidentes – define o processo de tratamento de incidentes de segurança através da execução de procedimentos e etapas bem definidos que conduzirão a Valloo ao retorno de suas normais atribuições através da resolução de um incidente.

iv. Política e Procedimentos do PCI-DSS – institui políticas e procedimentos para garantir a segurança dos dados de contas de pagamento e facilitar a adoção de medidas de segurança da informação de maneira geral a fim de garantir a conformidade com os requisitos do PCI-DSS v 4.0.

6. Responsabilidade e comunicação

O cumprimento desta Política é de responsabilidade de todos os colaboradores e prestadores de serviços, com a abrangência sobre as atividades que envolvam dados e informações no ambiente cibernético.

A alta administração da Valloo, compromete-se com a melhoria contínua dos procedimentos e controles relacionados nesta Política. Quaisquer indícios de incidentes ou irregularidades citadas nesta Política, devem ser comunicados imediatamente ao Comitê de Gestão da Valloo.

O treinamento em segurança cibernética é obrigatório para todos os colaboradores e fornecedores. O treinamento é baseado nas políticas e normas de segurança cibernética e é complementado por um programa de conscientização e sensibilização, que consiste de:

i. Iniciativas de sensibilização da cultura de segurança cibernética, incluindo a implementação de programas de treinamento e de avaliação periódica da sensibilização de colaboradores.

ii. Iniciativas de sensibilização sobre segurança cibernética para clientes, empresas terceiras e prestadores de serviços relevantes.

06_Política de Segurança Cibernética valloo.pdf

Documento número #40353578-2b87-4316-b273-f49f8e1cbc5e

Hash do documento original (SHA256): 598f544fabc2af5dde3d10e3285b1ed77397c063e4fd6b322ef1642de91a2050

Assinaturas

Luiza Araujo Chaves
Assinou em 29 abr 2025 às 15:53:10

Log

29 abr 2025, 11:55:56	Operador com email raquel.falsetti@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae criou este documento número 40353578-2b87-4316-b273-f49f8e1cbc5e. Data limite para assinatura do documento: 29 de maio de 2025 (11:55). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
29 abr 2025, 11:56:38	Operador com email raquel.falsetti@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae adicionou à Lista de Assinatura: luiza@valloo.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Luiza Araujo Chaves.
29 abr 2025, 15:53:10	Luiza Araujo Chaves assinou. Pontos de autenticação: Token via E-mail luiza@valloo.com.br. IP: 189.39.50.5. Localização compartilhada pelo dispositivo eletrônico: latitude -15.84105503218484 e longitude -47.85050529191971. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1190.0 disponibilizado em https://app.clicksign.com.
29 abr 2025, 15:53:12	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 40353578-2b87-4316-b273-f49f8e1cbc5e.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador 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