Abril de 2026

Título	Política de Segurança Cibernética
Número de referência	006
Número de versão	V 07
Status	Aprovada
Aprovador	Diretora Presidente
Data da aprovação	23/04/2026
Data da próxima revisão	23/04/2027
Área responsável	Diretoria Executiva de Infraestrutura e Seg. da Inform.
Normas externas e documentos relacionados	Resolução CMN nº 5274/2025 (publicada em dez/25)
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	10/02/2025	Diretoria Executiva de Infra e Segurança da Informação	Diretora Presidente	Revisão periódica
06	10/02/2025	Diretoria Executiva de Infra e Segurança da Informação	Diretora Presidente	Atualização da Resolução CMN 4.893/2021 com a Resolução CMN nº 5.274/2025, publicada em 18/12/2025

07	23/04/2026	Diretoria Executiva de Infra e Segurança da Informação	Diretora Presidente	Revisão Periódica

shis ql 22 conjunto 4 lote 19
lago sul . brasília/df
cep 71650.245

tel 55 61 3364.0005
valloo.com.br

Sumário

1. Objetivo

O objetivo desta política é estabelecer diretrizes, responsabilidades e requisitos mínimos para o gerenciamento da segurança cibernética garantindo a integridade, confidencialidade e disponibilidade de informações e dos sistemas utilizados pela Valloo, bem como promover a 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 regulatórios aplicáveis e a adequada gestão de riscos associados a terceiros. Essa polítiva deve ser seguida por todos os colaboradores, terceiros e prestadores de serviços com acesso, direto ou indireto, a qualquer tipo de dados, sistemas e informações 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 da Infraestrutura e Segurança da Informação a responsabilidade pela gestão da Segurança Cibernética bem como pela governança, implementação, supervisão e atualização desta Política.

3. Base Legal e Normativa

A Valloo segue os requerimentos da Resolução Resolução CMN nº 5.274/2025, publicada em 18/12/2025 eque 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. Essa resolução substituiu a CMN 4.893/2021 aprofundando e detalhando os controles mínimos obrigatórios.

4. Diretrizes Gerais de Segurança Cibernética

A Segurança Cibernética na Valloo deve ser tratada como parte integrante da governança corporativa, com foco em prevenção, detecção, resposta e recuperação frente a ameaças cibernéticas, visando reduzir a exposição a riscos operacionais, riscos reputacionais, riscos legais e impactos financeiros. A Área de Infraestrutura e Segurança da Informação é responsável pela criação, proposição, administração, supervisão e melhoria contínua de procedimentos e controles destinados a garantir que os riscos cibernéticos sejam identificados, avaliados, tratados e monitorados dentro dos limites de tolerância definidos pela organização.

Os programas e controles devem ser formalmente documentados, mantidos atualizados e revisados periodicamente, ao menos anualmente, ou sempre que ocorrerem mudanças relevantes no ambiente tecnológico, nos processos internos, na legislação aplicável ou após incidentes relevantes.

5. Procedimentos e Controles Mínimos para Segurança Cibernética

Em conformidade com a regulamentação vigente, a Valloo adota controles mínimos e procedimentos obrigatórios para garantir a proteção dos ambientes tecnológicos e das informações sob sua responsabilidade, incluindo, mas não se limitando a:

5.1. Controle de Acesso e Autenticação

- Implementação de mecanismos de autenticação forte, incluindo autenticação multifator (MFA) quando aplicável;
- Princípio do menor privilégio;
- Segregação de funções;
- Revisões periódicas de acessos;
- Controles específicos para acessos privilegiados e administrativos.

5.2. Proteção de Dados e Criptografia

- Criptografia de dados sensíveis em repouso e em trânsito;
- Proteção de chaves criptográficas e certificados digitais;
- Gestão segura do ciclo de vida de credenciais, chaves e certificados.

5.3. Monitoramento e Detecção de Ameaças

- Monitoramento contínuo de eventos de segurança;
- Registro e retenção adequada de logs para rastreabilidade e auditoria;
- Mecanismos de detecção e prevenção de intrusões;
- Controles de detecção de vazamento de dados e comportamentos anômalos.

5.4. Proteção contra Malware e Ameaças Persistentes

- Implementação de ferramentas de proteção contra malware, ransomware e ameaças persistentes avançadas;
- Atualização contínua de assinaturas e mecanismos de defesa;
- Controles adicionais de proteção para endpoints e servidores críticos.

5.5. Gestão de Vulnerabilidades e Correções

- Processo formal de gestão de vulnerabilidades, incluindo varreduras periódicas;
- Priorização e correção de vulnerabilidades conforme criticidade e risco;
- Controles para mitigação emergencial quando a correção imediata não for possível.

5.6. Testes de Intrusão e Avaliações Técnicas

- Execução de testes de intrusão (pentest) com periodicidade mínima anual ou sempre que houver mudanças relevantes no ambiente;
- Documentação formal dos resultados, evidências e plano de ação;

- Retenção dos registros e relatórios pelo período mínimo exigido pela regulamentação aplicável.

5.7. Gestão de Backup e Recuperação

- Política formal de backup e recuperação de dados;
- Garantia de integridade, segregação e proteção contra alterações indevidas;
- Testes periódicos de restauração para assegurar efetividade do processo.

5.8. Proteção de Infraestrutura e Redes

- Segmentação de redes e proteção de perímetros;
- Hardening de sistemas operacionais, bancos de dados e aplicações;
- Gestão de patches e configurações seguras;
- Controle de dispositivos e ativos conectados à rede.

5.9. Segurança de Integrações e APIs

- Implementação de controles específicos para integrações sistêmicas e APIs;
- Validação de autenticação, autorização e integridade de transações;
- Monitoramento de tráfego e proteção contra abuso de APIs.

5.10. Inteligência e Gestão Proativa de Ameaças

A Valloo deverá manter práticas de monitoramento de ameaças cibernéticas e tendências do setor, incluindo mecanismos que permitam identificar riscos emergentes, campanhas de fraude, vazamentos e exposição de credenciais, sempre que aplicável.

6. Segurança em Ambientes Críticos e Comunicação Eletrônica de Dados

A Valloo adotará controles reforçados e medidas específicas para ambientes considerados críticos, incluindo aqueles relacionados à comunicação eletrônica de dados e integrações com sistemas do Sistema Financeiro Nacional, tais como ambientes associados ao Pix, STR e demais infraestruturas críticas.

Tais controles incluem, quando aplicável:

- segregação lógica e física dos ambientes;
- autenticação multifator obrigatória para acessos privilegiados;
- gestão reforçada de credenciais, certificados e chaves criptográficas;
- validação de integridade de informações e transações;
- monitoramento contínuo e alertas para eventos suspeitos.

7. Contratação e Gestão de Serviços de Terceiros e Computação em Nuvem

A contratação de serviços de processamento e armazenamento de dados, inclusive serviços em nuvem, deverá observar requisitos mínimos de segurança e governança, contemplando:

- análise de riscos antes da contratação;
- avaliação de capacidade técnica, reputação e controles do fornecedor;
- definição de níveis de serviço (SLA) e obrigações de segurança;
- exigência de requisitos de confidencialidade e proteção de dados;
- previsão contratual de auditoria, acesso a evidências e controles;
- definição de responsabilidades e obrigações quanto a incidentes de segurança;
- exigência de continuidade de negócios e plano de recuperação de desastres;
- critérios formais para encerramento do contrato e descarte seguro de dados.

A Valloo assegurará que prestadores de serviço relevantes adotem controles compatíveis com os requisitos desta Política e com as obrigações regulatórias aplicáveis.

8. Tratamento de Incidentes de Segurança Cibernética

A Valloo mantém Plano de Resposta a Incidentes, com procedimentos formalizados para prevenção, identificação, contenção, erradicação, recuperação e lições aprendidas. Incidentes e indícios relevantes devem ser comunicados imediatamente à Área de Infraestrutura e Segurança da Informação, que será responsável por coordenar a resposta, registrar evidências e garantir que ações corretivas e preventivas sejam implementadas. Sempre que aplicável, serão observados requisitos de comunicação e reporte às autoridades competentes, clientes e demais partes interessadas, conforme legislação e regulamentação vigente.

9. Conscientização e Treinamento

O treinamento em Segurança Cibernética é obrigatório para todos os colaboradores e fornecedores relevantes, devendo ocorrer periodicamente e ser atualizado conforme mudanças tecnológicas, ameaças emergentes e requisitos regulatórios. O programa de conscientização inclui, no mínimo:

a. iniciativas de fortalecimento da cultura de segurança cibernética, incluindo treinamentos e avaliações periódicas de conhecimento;
b. iniciativas de conscientização para clientes, terceiros e prestadores de serviços relevantes, quando aplicável.

10. Responsabilidades e Comunicação

O cumprimento desta Política é responsabilidade de todos os colaboradores e prestadores de serviços, dentro do escopo de suas atribuições. A Alta Administração da Valloo compromete-se com a melhoria contínua dos controles e procedimentos relacionados à Segurança Cibernética, assegurando suporte institucional e recursos adequados para sua implementação. Quaisquer indícios de incidentes, irregularidades ou violações desta Política devem ser comunicados imediatamente à Diretoria de Infraestrutura e Segurança da Informação.

11. Políticas Complementares

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 Tecnologia S.A publicou as seguintes políticas que devem ser compreendidas como complementares à esse documento:

- 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;
- Política de Gestão de Ativos – institui procedimentos para a utilização, manutenção e gestão de ativos da empresa, visando proteger a integridade e confidencialidade do negócio;
- 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 empresa ao retorno de suas normais atribuições através da resolução de um incidente;
- Política e procedimentos do PCI-DSS – institui políticas e procedimentos para garantir a segurança dos dados de contas de cartões 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

12. Revisão e Atualização

Esta Política deve ser revisada no mínimo anualmente, ou a qualquer tempo quando houver:

- alterações regulatórias relevantes;
- mudanças significativas no ambiente tecnológico;
- mudanças na estrutura organizacional;
- incidentes de segurança relevantes;
- alterações significativas em serviços terceirizados e ambientes em nuvem.

06_Política de Segurança Cibernética valloo_2026 (1).pdf

Documento número #e8e3a544-31cf-4954-9698-1c594973edef

Hash do documento original (SHA256): 3ea506a9db1c275f31832cb63ce4552460cb3d16bc4988b5e8038abc092caab5

Assinaturas

Luiz Watanabe
CPF: 013.193.988-20
Assinou em 18 mai 2026 às 17:27:07

Bruno Pisciotta
CPF: 872.803.701-44
Assinou em 15 mai 2026 às 09:40:27

Raquel A. de Campos Falsetti
CPF: 195.290.208-80
Assinou em 15 mai 2026 às 09:55:36

Luiza Araujo Chaves
Assinou em 15 mai 2026 às 09:55:52

Maria Portela
CPF: 012.337.991-18
Assinou em 15 mai 2026 às 10:22:15

Marcela Duarte
CPF: 611.632.281-68
Assinou em 15 mai 2026 às 12:14:23

Fellipe Torres
CPF: 703.790.841-04
Assinou em 18 mai 2026 às 17:22:45

Log

15 mai 2026, 09:31:50	Operador com email eduardo.sousa@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae criou este documento número e8e3a544-31cf-4954-9698-1c594973edef. Data limite para assinatura do documento: 14 de junho de 2026 (09:30). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
15 mai 2026, 09:37:29	Operador com email eduardo.sousa@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.
15 mai 2026, 09:37:29	Operador com email eduardo.sousa@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae adicionou à Lista de Assinatura: fellipe.torres@valloo.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Fellipe Torres.
15 mai 2026, 09:37:29	Operador com email eduardo.sousa@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae adicionou à Lista de Assinatura: luiz.watanabe@valloo.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Luiz Watanabe.
15 mai 2026, 09:37:29	Operador com email eduardo.sousa@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae adicionou à Lista de Assinatura: maria.portela@valloo.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Maria Portela.
15 mai 2026, 09:37:29	Operador com email eduardo.sousa@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae adicionou à Lista de Assinatura: raquel.falsetti@valloo.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Raquel A. de Campos Falsetti e CPF 195.290.208-80.
15 mai 2026, 09:37:29	Operador com email eduardo.sousa@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae adicionou à Lista de Assinatura: marcela.duarte@valloo.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Marcela Duarte.
15 mai 2026, 09:37:29	Operador com email eduardo.sousa@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae adicionou à Lista de Assinatura: bruno.pisciotta@valloo.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; endereço de IP. Dados informados pelo Operador para validação do signatário: nome completo Bruno Pisciotta.
15 mai 2026, 09:40:27	Bruno Pisciotta assinou. Pontos de autenticação: Token via E-mail bruno.pisciotta@valloo.com.br. CPF informado: 872.803.701-44. IP: 177.207.235.157. Componente de assinatura versão 1.1442.0 disponibilizado em https://app.clicksign.com.

15 mai 2026, 09:55:36	Raquel A. de Campos Falsetti assinou. Pontos de autenticação: Token via E-mail raquel.falsetti@valloo.com.br. CPF informado: 195.290.208-80. IP: 177.207.235.157. Localização compartilhada pelo dispositivo eletrônico: latitude -15.841109 e longitude -47.85024599999999. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1442.0 disponibilizado em https://app.clicksign.com.
15 mai 2026, 09:55:52	Luiza Araujo Chaves assinou. Pontos de autenticação: Token via E-mail luiza@valloo.com.br. IP: 177.207.235.157. Localização compartilhada pelo dispositivo eletrônico: latitude -15.841109 e longitude -47.85024599999999. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1442.0 disponibilizado em https://app.clicksign.com.
15 mai 2026, 10:22:15	Maria Portela assinou. Pontos de autenticação: Token via E-mail maria.portela@valloo.com.br. CPF informado: 012.337.991-18. IP: 177.207.235.157. Componente de assinatura versão 1.1442.0 disponibilizado em https://app.clicksign.com.
15 mai 2026, 12:14:23	Marcela Duarte assinou. Pontos de autenticação: Token via E-mail marcela.duarte@valloo.com.br. CPF informado: 611.632.281-68. IP: 177.207.235.157. Componente de assinatura versão 1.1442.0 disponibilizado em https://app.clicksign.com.
18 mai 2026, 17:22:45	Fellipe Torres assinou. Pontos de autenticação: Token via E-mail fellipe.torres@valloo.com.br. CPF informado: 703.790.841-04. IP: 177.207.235.157. Componente de assinatura versão 1.1443.0 disponibilizado em https://app.clicksign.com.
18 mai 2026, 17:27:07	Luiz Watanabe assinou. Pontos de autenticação: Token via E-mail luiz.watanabe@valloo.com.br. CPF informado: 013.193.988-20. IP: 179.118.179.203. Localização compartilhada pelo dispositivo eletrônico: latitude -23.60726641729362 e longitude -46.73545371056911. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1443.0 disponibilizado em https://app.clicksign.com.
18 mai 2026, 17:27:08	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número e8e3a544-31cf-4954-9698-1c594973edef.