Agosto de 2026

Título	Política de Segurança da Informação
Número de referência	002
Número de versão	V 08
Status	Aprovada
Aprovador	Diretor Presidente
Data da aprovação	13/08/2026
Data da próxima revisão	13/08/2027
Área responsável	Diretoria Executiva de Segurança da Informação e Infraestrutura
Normas externas e documentos relacionados	Lei 13.709/2018, Resolução CMN 4.893/2021 e Resolução BCB 85/2021
Normas internas relacionadas	Política de Risco Operacional, Política de Segurança Cibernética, Plano de Ação e Resposta a Incidentes e Política de Segurança da Informação e Controles PCI DSS

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
05	25/06/2024	Área de Governança, Riscos e Compliance	CEO	Atualização de revisão de política
06	27/12/2024	Diretoria Executiva de Governança, Risco e Compliance	Diretora Presidente	Assinatura da Diretora Presidente
07	28/05/2025	Diretoria Executiva de	Diretora	Revisão Periódica

		Segurança da Informação e Infraestrutura	Presidente	
08	11/08/2026	Diretoria Executiva de Segurança da Informação e Infraestrutura	Diretor Presidente	Revisão Periódica

Sumário

1 Objetivo

Esta Política estabelece os princípios, diretrizes, responsabilidades e requisitos para a proteção das informações, dos dados, dos sistemas, dos recursos tecnológicos e dos demais ativos de informação da Valloo.

A Política tem como objetivo preservar a confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade e proteção das informações, assegurando que os riscos de segurança da informação e segurança cibernética sejam identificados, avaliados, tratados e monitorados de forma compatível com os objetivos estratégicos, o modelo de negócio, o perfil de risco e os requisitos legais, regulatórios e contratuais aplicáveis à Valloo.

A Política também estabelece as diretrizes para prevenção, detecção, resposta e recuperação diante de eventos e incidentes de segurança da informação e segurança cibernética, contribuindo para a resiliência operacional e a continuidade dos serviços prestados pela Valloo.

2 Abrangência

Esta Política aplica-se a:

- Valloo Tecnologia;
- Valloo Benefícios;
- Valloo Digital;
- Valloo Instituição de Pagamento;
- administradores, diretores e gestores;
- colaboradores e estagiários;
- prestadores de serviços e terceiros;
- fornecedores e parceiros de negócio;
- usuários internos e externos que tenham acesso a informações ou recursos da Valloo;
- todos os sistemas, aplicações, ambientes computacionais, redes, dispositivos, serviços em nuvem, bancos de dados e demais ativos de informação sob responsabilidade ou custódia da Valloo.

A Política aplica-se independentemente da localização física dos ativos ou da forma de armazenamento, processamento ou transmissão das informações.

3 Base Legal

A Valloo estabelece e mantém esta Política considerando, conforme sua aplicabilidade:

3.1 Legislação e regulamentação

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD);
- Lei nº 12.865/2013 e demais normas aplicáveis às instituições de pagamento;

- regulamentação vigente do Banco Central do Brasil relacionada à segurança cibernética;
- Resolução BCB nº 85/2021 e suas alterações;
- demais normas, circulares, resoluções, instruções normativas e atos regulamentares aplicáveis às atividades da Valloo;
- requisitos contratuais, legais e regulatórios aplicáveis aos serviços, produtos, clientes e parceiros da Valloo.

A Valloo deverá manter o acompanhamento das alterações legais e regulatórias que possam impactar esta Política e os controles de segurança da informação.

3.2 Normas e boas práticas

Esta Política considera como referências:

- ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação;
- ISO/IEC 27002 – Controles de Segurança da Informação;
- ISO/IEC 27005 – Gestão de Riscos de Segurança da Informação;
- ISO/IEC 27701, quando aplicável, para gestão de informações relacionadas à privacidade;
- PCI DSS e demais padrões aplicáveis aos ambientes de pagamento;
- frameworks e boas práticas reconhecidos de segurança cibernética e gestão de riscos.

A adoção dessas referências não implica certificação ou declaração de conformidade com determinada norma, salvo quando formalmente obtida ou declarada pela Valloo.

4 Princípios de Segurança da Informação

A Valloo adota os seguintes princípios:

4.1 A informação é um ativo corporativo e deve ser protegida durante todo o seu ciclo de vida.

4.2 A segurança da informação deve estar integrada aos processos de negócio e ser considerada desde o planejamento de novos produtos, serviços, processos, sistemas e tecnologias.

4.3 Os controles de segurança devem ser proporcionais à criticidade dos ativos, à sensibilidade das informações, aos riscos identificados e aos impactos potenciais para a Valloo, seus clientes, parceiros e demais partes interessadas.

4.4 A proteção da informação deve considerar, no mínimo, os princípios de:

- confidencialidade;
- integridade;
- disponibilidade;
- autenticidade;

- rastreabilidade;
- não repúdio, quando aplicável;
- proteção de dados pessoais;
- conformidade legal, regulatória e contratual.

4.5 O acesso às informações e aos recursos tecnológicos deve observar os princípios de necessidade de conhecimento, menor privilégio, segregação de funções e responsabilidade individual.

4.6 Os riscos de segurança da informação e segurança cibernética devem ser identificados, avaliados, tratados e monitorados de forma contínua.

4.7 Os controles de segurança devem ser continuamente aprimorados considerando mudanças tecnológicas, novas ameaças, incidentes, vulnerabilidades, resultados de auditorias, testes e avaliações de risco.

5 Governança e Responsabilidades

5.1 Alta Administração

A Diretoria da Valloo é responsável por assegurar que a segurança da informação e a segurança cibernética sejam tratadas de forma compatível com os objetivos estratégicos, o perfil de risco e os requisitos regulatórios aplicáveis.

Compete à Alta Administração:

- aprovar esta Política e suas revisões;
- assegurar recursos adequados para sua implementação;
- acompanhar os riscos relevantes de segurança da informação;
- acompanhar indicadores e relatórios de segurança;
- assegurar a implementação de medidas para tratamento de riscos relevantes;
- promover uma cultura organizacional de segurança da informação.

5.2 Diretor Responsável pela Segurança Cibernética e da Informação

A Valloo Instituição de Pagamento deve manter formalmente designado o diretor responsável pelas obrigações relacionadas à Política de Segurança Cibernética e da Informação e ao Plano de Ação e Resposta a Incidentes de Segurança, conforme regulamentação do Banco Central do Brasil.

O responsável deve possuir autoridade e recursos compatíveis com suas atribuições e não poderá exercer função que gere conflito de interesses.

5.3 Segurança da Informação

A área responsável por Segurança da Informação deve:

- estabelecer e manter controles de segurança;

- coordenar a gestão de riscos de segurança da informação;
- acompanhar vulnerabilidades e ameaças;
- coordenar o tratamento de incidentes;
- promover avaliações e testes de segurança;
- acompanhar a conformidade dos controles;
- apoiar auditorias internas e externas;
- promover treinamentos e campanhas de conscientização;
- manter normas, procedimentos e padrões técnicos relacionados à segurança.

5.4 Tecnologia da Informação

A área de Tecnologia deve implementar e operar os controles de segurança aplicáveis à infraestrutura, sistemas, redes, aplicações, ambientes cloud, dispositivos, bancos de dados e demais recursos tecnológicos.

5.5 Gestores das Informações

Cada informação relevante deve possuir responsável formalmente definido, que deve:

- determinar ou apoiar sua classificação;
- definir os requisitos de acesso;
- avaliar os riscos relacionados à informação;
- assegurar o tratamento adequado durante seu ciclo de vida;
- definir requisitos de retenção e descarte, em conjunto com as áreas responsáveis.

5.6 Usuários

Todos os usuários são responsáveis por:

- proteger as informações sob sua responsabilidade;
- utilizar os recursos corporativos exclusivamente para finalidades autorizadas;
- proteger suas credenciais;
- cumprir esta Política e as normas complementares;
- comunicar imediatamente eventos ou suspeitas de incidentes;
- não compartilhar informações com pessoas não autorizadas.

5.7 Terceiros

Terceiros e prestadores de serviços que tenham acesso a informações ou ativos da Valloo devem cumprir os requisitos de segurança estabelecidos contratualmente e nesta Política.

6 Gestão de Riscos de Segurança da Informação

A Valloo deve manter processo formal de identificação, análise, avaliação e tratamento dos riscos relacionados à segurança da informação e segurança cibernética.

A avaliação de riscos deve considerar, entre outros:

- ameaças internas e externas;
- vulnerabilidades;
- probabilidade de ocorrência;
- impacto financeiro;
- impacto operacional;
- impacto regulatório;
- impacto sobre clientes;
- impacto sobre dados pessoais;
- impacto reputacional;
- impacto sobre a continuidade dos serviços.

Os riscos identificados devem possuir tratamento definido, podendo incluir mitigação, transferência, aceitação ou eliminação, conforme critérios corporativos de gestão de riscos.

Riscos acima dos níveis de tolerância definidos pela Valloo devem ser formalmente comunicados e tratados pela autoridade competente.

7 Gestão de Ativos

A Valloo deve manter inventário atualizado dos ativos de informação relevantes, incluindo, conforme aplicável:

- servidores;
- dispositivos de rede;
- equipamentos de segurança;
- aplicações;
- bancos de dados;
- serviços cloud;
- contas e identidades;
- certificados e chaves criptográficas;
- sistemas de terceiros;
- informações corporativas;
- dados pessoais;
- dados relacionados a pagamentos;
- demais ativos críticos para o negócio.

Os ativos devem possuir responsáveis definidos e classificação de criticidade compatível com sua importância para o negócio.

8 Classificação e Tratamento da Informação

A informação deve ser classificada considerando sua sensibilidade, criticidade, valor para o negócio, requisitos legais e regulatórios e impacto decorrente de acesso, alteração, divulgação, perda ou indisponibilidade não autorizados.

A Valloo adota, no mínimo, as seguintes classificações:

8.1 Pública

Informação autorizada para divulgação pública, cujo acesso por terceiros não autorizados não represente impacto relevante para a Valloo.

8.2 Interna

Informação destinada ao uso interno da Valloo e que não deve ser divulgada externamente sem autorização. Informação cujo acesso, alteração, divulgação ou perda não autorizados possa causar impacto relevante à Valloo, seus clientes, parceiros, colaboradores ou demais partes interessadas.

8.3 Confidencial

Informação de elevada sensibilidade, cujo acesso deve ser limitado a pessoas expressamente autorizadas e cuja divulgação, alteração, perda ou acesso indevido possa resultar em impactos críticos, incluindo informações reguladas, credenciais privilegiadas, chaves criptográficas, informações financeiras, informações de segurança, dados pessoais sensíveis e informações relacionadas ao ambiente de dados de cartão, quando aplicável.

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.

Informações pessoais devem adicionalmente ser tratadas de acordo com os requisitos da LGPD e demais normas aplicáveis.

9 Gestão de Identidade e Controle de Acesso

A Valloo deve implementar controles destinados a assegurar que o acesso às informações e aos recursos tecnológicos seja concedido exclusivamente a usuários autorizados.

Os controles devem considerar, no mínimo:

- identificação individual dos usuários;
- autenticação adequada ao risco;
- princípio do menor privilégio;
- necessidade de conhecimento;
- segregação de funções;
- revisão periódica dos acessos;
- processo de concessão, alteração e revogação;
- controle de acessos privilegiados;
- autenticação multifator quando aplicável;
- rastreabilidade das atividades relevantes;

- gestão do ciclo de vida das identidades.

Contas compartilhadas devem ser evitadas e somente poderão existir quando tecnicamente justificadas e submetidas a controles compensatórios e mecanismos de rastreabilidade e utilizadas somente em perfis de consulta, não se admitindo o uso para execução de atividades de inclusão, alteração, exclusão e de qualquer natureza que implique o envio de dados para parceiros.

Acessos de colaboradores desligados ou terceiros cujo contrato tenha sido encerrado devem ser revogados de forma tempestiva.

10 Segurança de Infraestrutura, Redes e Computação em Nuvem

Os ambientes tecnológicos da Valloo devem ser protegidos por controles compatíveis com sua criticidade e exposição.

Devem ser considerados, conforme aplicável:

- segmentação de redes;
- firewalls e controles de tráfego;
- WAF;
- IDS/IPS;
- proteção contra malware;
- hardening;
- configuração segura de sistemas;
- criptografia;
- monitoramento;
- proteção de endpoints;
- gestão de vulnerabilidades;
- backup;
- mecanismos de alta disponibilidade;
- controles de acesso administrativo;
- mecanismos de detecção e prevenção de vazamento de informações.

Os ambientes de computação em nuvem devem ser submetidos aos mesmos princípios de segurança aplicáveis aos demais ambientes da Valloo, considerando também os riscos decorrentes do modelo de responsabilidade compartilhada.

A contratação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem deve observar os requisitos regulatórios aplicáveis, os critérios corporativos de gestão de riscos e os procedimentos de avaliação e contratação de terceiros.

11 Gestão de Vulnerabilidades e Atualizações

Os ambientes tecnológicos da Valloo devem ser protegidos por controles compatíveis com

sua criticidade e exposição.

A Valloo deve manter processo contínuo de identificação, avaliação, priorização e tratamento de vulnerabilidades.

Devem ser considerados:

- criticidade do ativo;
- severidade da vulnerabilidade;
- exposição do ativo;
- existência de exploração conhecida;
- criticidade do serviço;
- impacto para o negócio;
- existência de medidas compensatórias.

A Valloo deve estabelecer prazos de tratamento compatíveis com a criticidade dos riscos identificados.

Quando uma vulnerabilidade não puder ser corrigida dentro do prazo estabelecido, deverá ser formalmente registrada, avaliada quanto ao risco residual e submetida à aprovação da autoridade competente, podendo ser adotados controles compensatórios.

12 Segurança no Desenvolvimento e Mudanças

A segurança deve ser considerada durante todo o ciclo de desenvolvimento e manutenção de sistemas.

Os processos de desenvolvimento e alteração de sistemas devem contemplar, conforme aplicável:

- requisitos de segurança;
- análise de riscos;
- revisão de código;
- gestão de dependências;
- testes de segurança;
- análise de vulnerabilidades;
- segregação entre ambientes;
- controle de mudanças;
- proteção de informações utilizadas em desenvolvimento e testes;
- gestão segura de segredos e credenciais;
- aprovação antes da implantação em produção.

Sistemas desenvolvidos ou adquiridos de terceiros também devem ser submetidos aos requisitos de segurança definidos pela Valloo, de acordo com sua criticidade.

13 Criptografia e Gestão de Chaves

Informações classificadas como confidenciais ou restritas devem ser protegidas por mecanismos de criptografia quando requerido pelo risco, pela legislação, regulamentação, contrato ou padrão técnico aplicável.

A Valloo deve estabelecer controles para:

- geração de chaves;
- armazenamento;
- distribuição;
- utilização;
- rotação;
- revogação;
- backup, quando aplicável;
- destruição segura das chaves criptográficas.

Chaves criptográficas e credenciais privilegiadas devem receber proteção compatível com sua criticidade.

14 Registro, Monitoramento e Rastreabilidade

A Valloo deve manter mecanismos de registro e monitoramento capazes de detectar eventos relevantes de segurança e permitir a investigação de ocorrências.

Os registros devem ser protegidos contra alteração ou exclusão não autorizada e mantidos pelo período definido pela legislação, regulamentação, requisitos contratuais e critérios de segurança.

Devem ser monitorados, conforme aplicável:

- autenticações;
- acessos privilegiados;
- alterações de configuração;
- eventos de segurança;
- atividades administrativas;
- eventos relacionados a sistemas críticos;
- tentativas de acesso não autorizado;
- eventos relevantes de rede e infraestrutura.

15 Gestão de Incidentes de Segurança da Informação

A Valloo deve manter processo formal de identificação, registro, classificação, análise, contenção, erradicação, recuperação e encerramento de incidentes.

O processo deve contemplar:

- identificação e classificação do incidente;
- definição de responsabilidades;
- comunicação interna;

- preservação de evidências;
- contenção;
- investigação;
- recuperação;
- análise de causa;
- implementação de ações corretivas;
- registro das lições aprendidas.

Incidentes relevantes devem ser comunicados às partes internas e externas competentes, incluindo autoridades regulatórias, clientes, parceiros ou titulares de dados, quando exigido pela legislação, regulamentação ou contrato.

A Valloo deve manter Plano de Ação e Resposta a Incidentes formalmente documentado, aprovado e atualizado.

16 Continuidade de Negócios e Resiliência Cibernética

Os processos e serviços críticos devem possuir mecanismos destinados a assegurar sua continuidade e recuperação diante de falhas, indisponibilidades, incidentes de segurança ou eventos de desastre.

Devem ser considerados, conforme aplicável:

- backup e restauração;
- redundância;
- recuperação de ambientes;
- planos de contingência;
- procedimentos de disaster recovery;
- definição de RTO e RPO;
- testes periódicos;
- cenários de indisponibilidade decorrente de incidentes cibernéticos;
- dependências de terceiros e serviços cloud.

Os resultados dos testes devem ser documentados e as deficiências identificadas devem possuir planos de tratamento.

17 Segurança e Gestão de Terceiros

A contratação e gestão de terceiros que tenham acesso a informações, sistemas ou ambientes da Valloo devem considerar os riscos de segurança associados ao serviço.

A avaliação de terceiros deve considerar, conforme aplicável:

- criticidade do serviço;
- sensibilidade das informações;
- capacidade técnica;
- controles de segurança;

- certificações;
- relatórios de auditoria;
- histórico de incidentes;
- continuidade do serviço;
- subcontratação;
- localização e tratamento dos dados;
- requisitos regulatórios;
- capacidade de resposta a incidentes.

Contratos relevantes devem estabelecer, conforme aplicável:

- requisitos de segurança;
- confidencialidade;
- proteção de dados;
- responsabilidades;
- níveis de serviço;
- notificação de incidentes;
- direito de auditoria;
- requisitos de continuidade;
- requisitos de subcontratação;
- devolução ou eliminação de dados;
- requisitos para encerramento do serviço.

A responsabilidade da Valloo pela segurança, confidencialidade, integridade e disponibilidade das informações não é transferida ao prestador de serviço em decorrência da terceirização.

18 Privacidade e Proteção de Dados Pessoais

O tratamento de dados pessoais deve observar a legislação aplicável, especialmente a LGPD.

A Valloo deve implementar medidas técnicas e administrativas destinadas a proteger dados pessoais contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou tratamento inadequado.

Os requisitos de segurança e privacidade devem ser considerados desde a concepção de produtos, serviços, sistemas e processos.

Devem ser observados, conforme aplicável:

- finalidade e necessidade;
- minimização de dados;
- controle de acesso;
- proteção durante armazenamento e transmissão;
- retenção e descarte;

- gestão de incidentes envolvendo dados pessoais;
- gestão de terceiros e operadores;
- atendimento aos direitos dos titulares;
- registros e evidências de conformidade.

As responsabilidades específicas relacionadas à privacidade, proteção de dados e atuação do Encarregado devem ser definidas nos documentos corporativos correspondentes.

19 Segurança do Ambiente de Dados de Cartão – PCI DSS

A Valloo reconhece os requisitos do PCI DSS como requisitos específicos e complementares para proteção dos dados de cartão e do ambiente de dados de cartão sob sua responsabilidade.

Os controles relacionados aos 12 requisitos do PCI DSS são estabelecidos e detalhados na Política de Segurança da Informação e Controles PCI DSS da Valloo.

Essa política é parte integrante do conjunto de políticas e normas de segurança da informação da Valloo e deve ser observada conjuntamente com esta Política.

Quando houver conflito entre esta Política e requisitos específicos do PCI DSS, deverão ser aplicados os requisitos mais restritivos, salvo quando formalmente definido e documentado pela área responsável, considerando os requisitos de conformidade aplicáveis.

Os procedimentos, padrões técnicos e evidências relacionados ao PCI DSS devem ser mantidos conforme os requisitos do padrão, do ambiente de dados de cartão e das avaliações de conformidade realizadas pela Valloo.

20 Gestão de Pessoas e Conscientização

A Valloo deve promover cultura de segurança da informação por meio de programas permanentes de conscientização e capacitação.

Os programas devem abordar, conforme aplicável:

- proteção de credenciais;
- phishing e engenharia social;
- proteção de informações;
- LGPD;
- uso aceitável dos recursos corporativos;
- segurança cibernética;
- comunicação de incidentes;
- responsabilidades dos usuários;
- requisitos específicos das funções exercidas.

Colaboradores e terceiros devem conhecer suas responsabilidades de segurança antes de

receber acesso a informações ou recursos corporativos.

21 Segurança Física

Os ambientes físicos que armazenem ou processem informações ou suportem serviços críticos devem possuir controles de segurança física e ambiental compatíveis com os riscos identificados.

Devem ser considerados, conforme aplicável:

- controle de acesso físico;
- monitoramento;
- proteção contra incêndio;
- energia;
- temperatura;
- disponibilidade;
- proteção de equipamentos;
- descarte seguro de mídias e equipamentos.

22 Conformidade, Auditoria e Testes

A Valloo deve realizar avaliações periódicas da efetividade dos controles de segurança da informação e segurança cibernética.

Podem ser utilizados, conforme aplicável:

- auditorias internas;
- auditorias externas;
- testes de vulnerabilidade;
- testes de intrusão;
- avaliações de configuração;
- testes de continuidade;
- avaliações de terceiros;
- análises de conformidade;
- exercícios de resposta a incidentes.

Os resultados devem ser documentados e as deficiências identificadas devem ser tratadas por meio de planos de ação, considerando o risco e a criticidade.

As evidências relacionadas à Política de Segurança Cibernética, ao Plano de Ação e Resposta a Incidentes, aos relatórios e demais documentos regulatórios devem ser mantidas pelo período estabelecido pela regulamentação aplicável.

23 Indicadores de Segurança

A Valloo deve estabelecer indicadores para acompanhamento da efetividade de seu programa de segurança da informação.

Os indicadores podem incluir, entre outros:

- incidentes de segurança;
- vulnerabilidades críticas e de alto risco;
- prazo de correção de vulnerabilidades;
- disponibilidade de serviços críticos;
- cumprimento de planos de ação;
- acessos privilegiados;
- revisões de acesso;
- incidentes envolvendo terceiros;
- resultados de testes de segurança;
- resultados de testes de continuidade;
- participação em treinamentos;
- indicadores relacionados à conformidade regulatória e PCI DSS.

Os indicadores relevantes devem ser reportados à gestão e à Alta Administração em periodicidade definida.

24 Gestão de Exceções

Exceções aos requisitos desta Política somente poderão ocorrer quando houver justificativa formal e avaliação documentada dos riscos envolvidos.

A solicitação de exceção deve conter, no mínimo:

- requisito que não poderá ser atendido;
- justificativa;
- risco associado;
- impacto;
- controles compensatórios;
- prazo da exceção;
- responsável pelo tratamento;
- aprovação da autoridade competente.

Exceções devem possuir prazo definido e ser reavaliadas antes de sua renovação.

25 Documentos Complementares

Esta Política deve ser complementada por normas, procedimentos, padrões técnicos e políticas específicas.

Fazem parte da estrutura de governança de segurança da informação da Valloo, conforme aplicabilidade:

- Política de Segurança da Informação e Controles PCI DSS;
- Política de Gestão de Acessos;
- Política de Gestão de Riscos e Controles Internos;

- Plano de Resposta a Incidentes de Segurança;
- Política de Continuidade de Negócios;
- Política de Privacidade;
- Política de Fornecedores;
- Política de Uso Aceitável de Tecnologias Críticas;
- Política de Gestão de Ativos;
- Política de Gestão de Acessos;
- Política de Gestão de Mudanças;
- Política de Desenvolvimento Seguro;
- normas e padrões técnicos de segurança;
- demais documentos corporativos relacionados à segurança da informação.

Em caso de existência de requisitos específicos em normas, contratos ou regulamentações, estes devem ser incorporados aos documentos complementares aplicáveis.

26 Conscientização e Aceite

Todos os colaboradores, administradores, terceiros e demais usuários abrangidos por esta Política devem ter conhecimento de suas responsabilidades e obrigações relacionadas à segurança da informação.

A Valloo deve manter registros de treinamentos, comunicações e, quando aplicável, aceite formal desta Política.

O descumprimento desta Política poderá resultar na adoção de medidas administrativas, disciplinares, contratuais ou legais cabíveis.

27 Revisão e Aprovação

Esta Política deve ser revisada, no mínimo, anualmente e sempre que ocorrer:

- alteração relevante no modelo de negócio;
- alteração significativa no ambiente tecnológico;
- alteração legal ou regulatória relevante;
- mudança significativa no perfil de risco;
- ocorrência de incidente relevante;
- identificação de deficiência relevante nos controles;
- alteração relevante nas normas ou padrões adotados pela Valloo.

A Política de Segurança Cibernética e o Plano de Ação e Resposta a Incidentes da Valloo Instituição de Pagamento devem ser submetidos à aprovação da autoridade competente, conforme a estrutura de governança da instituição e a regulamentação do Banco Central do Brasil.

As versões aprovadas devem ser formalmente registradas e mantidas pelo prazo estabelecido pela regulamentação aplicável.

28 Disposições Finais

Esta Política estabelece os princípios e requisitos corporativos mínimos para a segurança da informação e segurança cibernética na Valloo.

Os controles específicos, procedimentos operacionais, configurações técnicas e responsabilidades detalhadas devem ser definidos nos documentos complementares correspondentes.

A existência desta Política não elimina a necessidade de implementação, operação, monitoramento, teste e melhoria contínua dos controles de segurança da informação.

A Valloo deve manter estrutura de governança capaz de demonstrar, por meio de documentos e evidências, a implementação e a efetividade dos controles estabelecidos nesta Política.