Fevereiro de 2023

Título	Política de Segurança Cibernética
Número de referência	006
Número de versão	V 03
Status	Aprovada
Aprovador	CEO
Data da aprovação	01/02/2023
Data da próxima revisão	01/02/2025
Área responsável	Presidência da Valloo Tecnologia
Normas externas e documentos relacionados	Resolução CMN 4.658/2018
Normas internas relacionadas	Política de Risco Operacional

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

Sumário

1. Objetivo

Estabelecer diretrizes e responsabilidades para o gerenciamento da segurança da informação cibernética e promover a melhoria contínua dos procedimentos relacionados com a segurança dos dados e informações, para prevenir, detectar e reduzir vulnerabilidades a incidentes relacionados com o ambiente cibernético, assim como possibilitar a manutenção da confidencialidade, da integridade e da disponibilidade das informações sob responsabilidade da Valloo.

2. Abrangência

Todos os administradores (Diretoria e demais gestores) e colaboradores das empresas ligadas e controladas pela Valloo.

3. Base Legal

A Valloo segue os requerimentos da Resolução CMN 4.658, 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 financeiras e demais instituições autorizadas a funcionar pelo Banco Central do Brasil.

4. Programa de Segurança da Informação

Os controles de segurança cibernética fornecem a base do Programa de Segurança da Informação, estabelecem as regras para proteger o ambiente de TI e estão amparados nos seguintes pilares de governança e melhores práticas:

4.1. Garantir a segurança e a confidencialidade das informações de clientes, parceiros, fornecedores e empregados;

4.2. Proteger contra ameaças ou riscos à segurança dessas informações;

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

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

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

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

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

5. Segurança Cibernética

A fim de reduzir a vulnerabilidade aos incidentes e cumprir os objetivos da segurança cibernética, a Área de Segurança da Informação da Valloo Tecnologia S.A. é responsável

pela criação, proposição, administração e supervisão de políticas e normas concebidas 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.

Os programas são documentados e atualizados anualmente para garantir a conformidade contínua com os requisitos regulamentares. A Valloo implementa a autenticação de usuários em plataforma tecnológica, requisitos de criptografia de dados sensíveis, prevenção e detecção de intrusão e de vazamento de informações, além da realização de testes e varreduras para detecção de vulnerabilidades.

A Norma de Gerenciamento de Identidade e Autenticação tem como principal objetivo o gerenciamento de identidades digitais para usuários, sistemas e processos, bem como na verificação de identidades que acessam recursos de TI da Valloo.

6. Plano de Monitoramento e Resposta a Incidentes

A identificação e a eliminação tempestiva de vulnerabilidades de tecnologia são fundamentais para garantir a integridade do ambiente dos processos de negócios. O Plano visa a descoberta de vulnerabilidades aplicáveis a Valloo, define processos que combinem o monitoramento contínuo para identificar os recursos afetados e a avaliação de riscos para determinar a priorização para a correção.

São estabelecidas as medidas de preparação, identificação, contenção, erradicação, recuperação e gestão do conhecimento gerado, além da definição de requisitos de monitoramento, resposta e responsabilidades.

7. Proteção contra softwares maliciosos

Estão definidos os requisitos de controle de detecção e prevenção para impedir que códigos maliciosos sejam executados e se infiltrem na rede da Valloo. Os mecanismos de proteção contra códigos maliciosos incluem, por exemplo, o monitoramento de atividades de *endpoints*.

A Valloo captura eventos relevantes para a identificação de possíveis incidentes de segurança cibernética (aqueles resultantes de atividades de intenção maliciosa). Os eventos são capturados e analisados pelo Centro de Operações de Segurança (SOC – Security Operations Center) da Valloo Tecnologia S.A. e utiliza serviços e ferramentas para monitorar e analisar os dados e alertas.

8. Controles de acesso e segmentação da rede de computadores

O programa de Gerenciamento de Identidade e Acesso implementa padrões e controles de acesso em toda a infraestrutura e aplicativos, especialmente aqueles que contêm informações de clientes. Esses controles são projetados para autenticar usuários, permitir acesso autorizado, garantir procedimentos administrativos consistentes, manter a segregação de funções e garantir atualizações tempestivas por meio de processos de inclusão, exclusão ou transferência nos sistemas da Valloo.

9. Manutenção de cópias de segurança dos dados e das informações

O backup operacional abrange proteção de dados em nível de arquivo, retenção de dados e recuperação de arquivos para atender aos requisitos de recuperação operacional e inclui backup de dados, restauração e validação de backup e recertificação.

10. Desenvolvimento de sistemas e adoção de novas tecnologias

A Valloo estabelece os requisitos de controle para o desenvolvimento de tecnologia, incluindo mudanças de software e configuração, independentemente da estrutura ou do modelo do ciclo de vida de desenvolvimento de software seguido pela equipe.

Esta norma se aplica aos softwares desenvolvidos pela Valloo Tecnologia S.A., incluindo alterações de configuração, e aos desenvolvedores associados a esse desenvolvimento

11. 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 comunicadas imediatamente para a Direção da Valloo Tecnologia.

O treinamento em segurança cibernética é obrigatório para todos os empregados. O treinamento é baseado nas políticas e normas de segurança cibernética e é complementado por um programa de conscientização.

06_Política de Segurança Cibernética valloo.pdf

Documento número #24b3d834-ae00-4eff-a2eb-f7f0379b961e

Hash do documento original (SHA256): c61574f52bfef6f50d7f8556931a012b17a11436740b560b30b3e38a138ee95f

Assinaturas

Luiza Araujo Chaves
Assinou em 02 jan 2025 às 16:16:51

Log

02 jan 2025, 11:16:51	Operador com email elizabeth.lessa@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae criou este documento número 24b3d834-ae00-4eff-a2eb-f7f0379b961e. Data limite para assinatura do documento: 01 de fevereiro de 2025 (11:16). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
02 jan 2025, 11:19:20	Operador com email elizabeth.lessa@valloo.com.br na Conta 14af7250-334e-483b-ac2e-afd001df00ae alterou o processo de assinatura. Data limite para assinatura do documento: 31 de janeiro de 2025 (11:16).
02 jan 2025, 11:19:21	Operador com email elizabeth.lessa@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.
02 jan 2025, 16:16:51	Luiza Araujo Chaves assinou. Pontos de autenticação: Token via E-mail luiza@valloo.com.br. IP: 177.207.235.157. Componente de assinatura versão 1.1086.1 disponibilizado em https://app.clicksign.com.
02 jan 2025, 16:16:53	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 24b3d834-ae00-4eff-a2eb-f7f0379b961e.