Politica de segurança cibernética

Valepay Brasil Ltda.

Versão: V1 – 10/10/2020

Status: Revisado

I. Objetivo

A Política de Segurança Cibernética visa garantir a proteção e a manutenção da privacidade, integridade, disponibilidade e confidencialidade das informações, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, de forma a proporcionar plena satisfação quanto à segurança e privacidade de suas informações.

II. Procedimentos e controles:

Para garantir a segurança da informação, estamos fundamentados nos princípios de segurança da informação, cujo objetivos constituem a preservação da propriedade da informação, notadamente sua confidencialidade, integridade e disponibilidade, permitindo o uso e compartilhamento de forma controlada, bem como o monitoramento e tratamento de incidentes provenientes de ataques cibernético.

Confidencialidade: Garantia de que a informação somente estará acessível para pessoas autorizadas;

Integridade: Garantia de que a informação, armazenada ou em trânsito, não sofrerá qualquer modificação não autorizada, seja esta intencional ou não;

Disponibilidade: Garantia de que a informação estará disponível sempre que for necessário.

2. Diretrizes gerais

O acesso às informações e aos ambientes tecnológicos da empresa é permitido apenas às pessoas autorizadas pelo proprietário da informação, levando em consideração o princípio do menor privilégio, a segregação de funções conflitantes e a classificação da informação. O controle de acesso aos sistemas deve ser formalizado e contemplar, no mínimo, os seguintes controles:

A utilização de identificadores (credencial de acesso) individualizados, monitorado e passíveis de bloqueios e restrições (automatizados e manuais);

Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pela Valepay

Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam a segurança das informações sensíveis.

3. Processo de segurança:

3.1. Os Ativos devem ser inventariados e protegidos de acessos indevidos ou ameaças que possam comprometer o negócio. Para tanto, o acesso às salas com documentos físicos deve ser limitado, por meio de mecanismos de autenticação e autorização de acesso.

3.2. Autenticação A Valepay adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

3.3. Segmentação de rede Valepay deve adotar mecanismos internos para a segmentação de rede para proteger seus dados de ataques cibernéticos e determinar que todos os computadores conectados à rede corporativa não estejam acessíveis diretamente pela Internet, seguindo as regras do firewall.

3.4. Classificação da Informação As informações devem ser classificadas segundo sua criticidade e sensibilidade para o negócio e seus clientes. Portanto, a Valepay deve adotar a seguinte classificação: -

Informação Pública: aquela que pode ser acessada por todos, sem restrição. São exemplos de Informação Pública: dados promocionais e publicidades;

Informação Interna: aquela que pode ser acessada somente por Colaboradores da Valepay. São exemplos de Informação Interna: normas, procedimentos, formulários e acesso ao sistema.

Informação Restrita: aquela que pode ser acessada somente por Colaboradores que precisam dela para desempenhar suas atribuições. São exemplos de Informação Restrita: Informações dos clientes e acesso ao sistema e informações sobre os clientes.

Informação Confidencial: aquela que pode ser acessada somente por Colaboradores que tenham permissão de acesso ou que necessitem dela para um propósito específico. São exemplos de Informação Confidencial: plano estratégico, contratos e desenvolvimento de novas tecnologias.

3.5. Gestão de riscos A Valepay possui processo para análise de vulnerabilidades, ameaças e impactos sobre os Ativos de informação para, diante de um incidente, adotar as medidas adequadas para minimizar os danos causados.

4 Backup e gravação de LOG

A Valepay deve adotar uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades. A Valepay também deve realizar gravação de logs de dados que permitam a rastreabilidade do acesso e a identificação do criador, data, meios de acesos e informações acessadas. As informações dos logs devem ser protegidas contra alterações e acessos não autorizados.

4.1. Proteção contra vírus, arquivos e softwares maliciosos A Valepay deve adotar mecanismos para prevenir que vírus e outros tipos de software e condutas maliciosas (e.g., phishing, spam etc.) se propaguem nos computadores, sistemas e servidores ou exponham a vulnerabilidades.

4.2. Testes de varredura para detecção de vulnerabilidade A Valepay deve promover monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

4.3. Criptografia Os Ativos de informação da Valepay devem possuir criptografia adequada, a fim de se garantir proteção em todo o ciclo de vida da informação, em conformidade com os padrões de segurança dos órgãos reguladores.

5. Plano de continuidade A Valepay realiza plano de continuidade dos serviços prestados a partir da adoção de um conjunto preventivo de estratégias e planos de ação para garantir que os serviços essenciais da Valepay sejam devidamente identificados e preservados após a ocorrência de uma contingência. Para tanto, realizará o mapeamento de processos críticos, análise de impacto nos negócios e inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança. Devem ser aplicados testes de continuidade de serviços de pagamento e realização testes periódicos para garantir a eficácia e segurança dos processos.

III. Gestão de incidentes

Todos os incidentes ou suspeita de incidentes identificados por um Colaborador, cliente, prestador de serviços, fornecedor, provedor ou parceiro devem ser imediatamente comunicados à área responsável. A comunicação deverá ser feita por meio dos canais indicados pela contato@valepay.com.br. Os incidentes reportados serão classificados

segundo o risco que representam para o impacto na continuidade dos negócios, eles devem ser devidamente registrados, tratados e comunicados.

IV. Treinamentos e conscientização

A Valepay preza por uma cultura de Segurança da Informação e Segurança Cibernética. Dessa forma, devem ser adotados políticas e procedimentos para a difusão dos princípios e diretrizes integrantes desta Política, garantindo-se a capacitação e conscientização para todos os seus Colaboradores. Semdp assim promoverá a ampla divulgação desta Política a todos os seus Colaboradores e o público em geral, bem como às empresas prestadoras de serviços a terceiros, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, incluindo a prestação de informações aos usuários finais sobre medidas de precaução para a utilização dos produtos e serviços oferecidos. Além disto, a Administração deverá difundir a cultura de Segurança da Informação e Segurança Cibernética para promover melhorias contínuas em seus processos internos, a fim de evitar quaisquer incidentes relacionado à Segurança da Informação e Segurança Cibernética

Contratação de serviços de processamento e armazenamento de dados e computação em nuvem

Os serviços de computação em nuvem disponibilizados, sob demanda e de maneira virtual, deverão incluir um ou mais serviços conforme descritos abaixo: - Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela Valepay ou por ela adquiridos.

A Valepay é responsável, em conjunto com o prestador de serviços, pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

V. Continuidade dos serviços de pagamento

No tocante à continuidade dos serviços de pagamento prestados, a Valepay deve assegurar:

- O tratamento dos incidentes relevantes relacionados com o ambiente cibernético;

- Os procedimentos a serem seguidos no caso de interrupção de serviços de processamento e armazenamento de dados e de computação em nuvem contratados,

abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal

- Os cenários de incidentes considerados nos testes de continuidade de serviços de pagamento prestados.

- O tratamento para mitigar os efeitos dos incidentes relevantes da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados;

- O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;

- Deve instituir mecanismos de acompanhamento e de controle visando a assegurar a implementação e a efetividade desta Política, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem. Os mecanismos de acompanhamento e controle devem incluir a definição de processos, testes e trilhas de auditoria, bem como a definição de métricas e indicadores adequados e a identificação e a correção de eventuais deficiências.

VI. DECLARAÇÃO DE RESPONSABILIDADE

Os Colaboradores e prestadores de serviço devem aderir formalmente a um termo em que se comprometem a agir de acordo com esta Política. Ademais, todos os contratos devem possuir cláusula que assegure a confidencialidade das informações.

DISPOSIÇÕES GERAIS Esta Política está acompanhada de um Termo de Adesão à Política de Segurança da Informação e Segurança Cibernética e Termo de Adesão às Alterações da Política de Segurança da Informação e Segurança Cibernética, que deverão ser assinados por todos os Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros.