



## **POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO**

### **1. OBJETIVO**

Estabelecer conceitos, diretrizes e responsabilidades sobre os principais aspectos relacionados à segurança cibernética e segurança da informação, visando preservar a confidencialidade, integridade, disponibilidade e conformidade de todas as informações sob gestão da CashWay. Definir os princípios fundamentais que formam a base da Política de Segurança Cibernética e da Informação, norteando a elaboração de normas, processos, padrões e procedimentos.

### **2. ABRANGÊNCIA**

Aplica-se a todas as áreas de Negócio da CashWay.

### **3. DIRETRIZES GERAIS**

A informação é um ativo essencial para os negócios de uma organização e sendo assim deve ser adequadamente protegida. Isto é especialmente importante em um ambiente de negócios cada vez mais interconectado.

Segurança cibernética e da informação é a proteção das informações contra diversos tipos de ameaças, para minimizar a exposição da empresa a riscos, garantindo que as características fundamentais da informação sejam preservadas, sendo elas: confidencialidade, integridade, disponibilidade e conformidade. Isso significa proteger a empresa contra o vazamento de informações, contra fraudes, zelar pela privacidade, garantir que sistemas e informações estejam disponíveis quando necessário e zelar pela proteção da imagem e das marcas da empresa.

A CashWay, através do departamento de Tecnologia da Informação e de forma alinhada com os objetivos e requisitos do negócio, estabelece nesta Política de Segurança Cibernética e da Informação, regras e direcionamentos a serem seguidos e aplicados a pessoas, processos e tecnologia, de forma a proteger as informações da CashWay, de seus clientes, fornecedores e parceiros de negócios.

### **3.1. DEFINIÇÕES**

Para efeito deste documento, aplicam-se os seguintes termos e definições:

#### **3.1.1. Recursos**

Qualquer recurso, tangível ou intangível, pertencentes, a serviço ou sob responsabilidade da CashWay, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.

#### **3.1.2. Ameaça**

Qualquer causa potencial de um incidente indesejado que possa resultar em impacto nos objetivos do negócio. As ameaças podem ser internas ou externas, intencionais ou não intencionais.

#### **3.1.3. Boas Práticas de Segurança da Informação**

São consideradas boas práticas de segurança da informação as recomendações contidas em normas e instituições como: ISO/IEC 27001, ISO/IEC 31000, OWASP ([www.owasp.org](http://www.owasp.org)), NIST ([www.nist.gov](http://www.nist.gov)), ISACA ([www.isaca.com.br](http://www.isaca.com.br)), SANS ([www.sans.org](http://www.sans.org)) e outras internacionalmente reconhecidas.

#### **3.1.4. Colaborador**

Entende-se como Colaborador qualquer pessoa que trabalhe para a CashWay quer seja: Funcionário com registro em carteira de trabalho, terceiro, estagiário, aprendiz ou *trainee*.

#### **3.1.5. Controle**

Qualquer recurso ou medida que assegure formas de tratamento de riscos, incluindo a redução, eliminação ou transferência. A implantação e manutenção adequada de controles materializa a segurança das informações. Podem ser interpretados como controles: políticas, processos, estruturas organizacionais, técnicas padrões, software, hardware e outros.

#### **3.1.6. Gestor**

*Colaborador que exerce cargo de liderança, como: presidente, vice-presidente, diretor, gerente, coordenador, líder ou chefe de seção.*

### **3.1.7. IDS**

*Intrusion Detection System* ou Sistema de Detecção de Intrusão é uma ferramenta utilizada para monitorar o tráfego da rede, detectar e alertar sobre ataques e tentativas de acessos indevidos.

### **3.1.8. IPS**

*Intrusion Prevention System* ou Sistema de Prevenção de Intrusão é uma ferramenta que tem a capacidade de identificar uma intrusão, analisar a relevância do evento/risco e bloquear determinados eventos, fortalecendo assim a tradicional técnica de detecção de intrusos.

### **3.1.9. Informação**

*Qualquer conjunto organizado de dados que possua algum propósito e valor para a CashWay, seus clientes, parceiros e colaboradores. A informação pode ser de propriedade da empresa, estar sob sua custódia ou sob custódia de terceiros, como por exemplo, informações armazenadas em nuvem.*

### **3.1.10. Princípios de “Least Privilege” e “Need to Know”**

*Estes princípios devem reger a autorização de qualquer acesso a sistemas e informações. Segundo eles, deve ser concedido apenas o nível mínimo de acesso (Least Privilege) a quem realmente tenha a necessidade de acesso (Need to Know).*

### **3.1.11. Política de Segurança Cibernética e da Informação**

*Estrutura de documentos formada pela Política, normas e padrões de segurança cibernética e segurança da informação.*

## **3.2. Risco**

*Qualquer evento que possa afetar a capacidade da companhia de atingir seus objetivos e sua estratégia de negócios ou, conforme a ISO 31000, o efeito da incerteza nos objetivos.*

## **3.3. Segurança da Informação (SI)**

Segurança da Informação é a proteção das informações, sendo caracterizada pela preservação de:

- **Confidencialidade:** garantia de que a informação somente será acessada por pessoas efetivamente autorizadas;
- **Integridade:** garantia de que o conteúdo da mensagem não será alterado ou violado indevidamente, ou seja, mede a exatidão da informação e seus métodos de modificação, manutenção e validade.

- **Disponibilidade:** garantia de que os Colaboradores autorizados obtenham acesso à informação e aos sistemas correspondentes sempre que necessários, nos períodos e ambientes aprovados pela empresa;
- **Conformidade:** Garantia de que controles de segurança da informação, devidamente estabelecidos, estão sendo executados conforme esperado e produzindo resultados efetivos no cumprimento de seus objetivos.

### 3.4. Segurança Cibernética

Conjunto de tecnologias, processos e práticas projetados para proteger redes, computadores, sistemas e dados de ataques, danos ou acesso não autorizado. Também conhecida como Segurança de TI, visa proteger somente assuntos relacionados ao digital.

### 3.5. Recursos Críticos

Recursos essenciais para o funcionamento da operação da CashWay e que possuem informações críticas ou sensíveis.

### 3.6. Baselines

Requisitos, recomendações e melhores práticas de configurações de segurança da informação para os ativos.

### 3.7. Nuvem (Cloud)

Infraestrutura, plataforma, aplicação ou serviço localizado na *internet*. A nuvem pode ser pública com acesso a todos, privada, com acesso restrito ou híbrido, com parte restrita e parte irrestrita.

### 3.8. IoT (Internet of Things – Internet das Coisas)

Conexão de dispositivos eletrônicos, como aparelhos eletrodomésticos, eletro portáteis, máquinas industriais, meios de transporte, dentre outros utilizados no dia-a-dia à internet.

## DIRETRIZES ESPECÍFICAS

### 3.9. Aquisição, Desenvolvimento e Manutenção de Tecnologia da Informação.

- i. Aquisições, desenvolvimento, contratações e a manutenções de Tecnologia da Informação devem ser centralizadas e gerenciadas pela área de Tecnologia da Informação.
- ii. Responsáveis pela aquisição de produtos ou serviços de Tecnologia da Informação, assim como o desenvolvimento e manutenção de ativos tecnológicos, devem:
  - Garantir a adoção e manutenção dos requisitos previamente definidos nos baselines, padrões e normas de segurança da informação;
  - Garantir a validação de requisitos de Segurança da Informação na análise crítica de novas soluções ou para aquelas que sofreram alterações significativas;

- Garantir o atendimento aos requisitos de segurança necessários para assegurar a confidencialidade, integridade, disponibilidade e conformidade de sistemas e informações.
  - Garantir que novas soluções sejam devidamente documentadas, assim como mantida documentação para entendimento e rastreabilidade das ações realizadas.
- iii. Os Recursos de Tecnologia da Informação utilizados pela CashWay devem ser inventariados, controlados e colocados à disposição de acordo com as regras de acesso vigentes e boas práticas de segurança da informação.
  - iv. Na contratação de serviços, os contratos firmados entre as partes e a CashWay devem conter cláusulas de confidencialidade, responsabilidade pela proteção da informação, não divulgação e descarte das informações. Outras cláusulas específicas de Segurança da Informação podem ser requeridas de acordo com o contexto do serviço contratado.
  - v. O sigilo necessário com as informações da CashWay deve perdurar mesmo após o encerramento da prestação de serviços. Este ponto deve ser previsto no estabelecimento de contratos.
  - vi. A veracidade das informações contidas em contratos deve ser verificada.
  - vii. Devem ser seguidas as boas práticas de segurança da informação no ciclo de desenvolvimento de sistemas da empresa.

### **3.10. Classificação da Informação**

- i. As informações devem ser atribuídas a um proprietário formalmente designado.
- ii. Toda a informação deve ser classificada, de acordo com seu valor, grau de sigilo, criticidade e sensibilidade perante o negócio, de forma que sejam adotados os mecanismos de proteção adequados, balanceando custo e complexidade do controle.
- iii. Informações sem classificação explícita devem ser consideradas como "Interno", não sendo permitido o seu repasse ou divulgação para qualquer pessoa que não seja da CashWay exceto informações públicas e de mercado, devidamente autorizadas.
- iv. Todos os Colaboradores devem tratar as informações da CashWay de acordo com seu nível de classificação de forma a protegê-las contra atos ou acessos indevidos ou divulgação não autorizada, mantendo sua confidencialidade, integridade e disponibilidade.

### **3.11. Comportamento Seguro**

- i. Os recursos e as informações de propriedade ou sob custódia da CashWay devem ser utilizados de acordo com os interesses da organização, para prestação dos seus serviços, atendendo aos requisitos e respeitando as regras estabelecidas.

- ii. Independente dos meios onde a informação esteja armazenada, ou seja, transmitida, cada Colaborador deve assumir um comportamento seguro e proativo impedindo seu vazamento para pessoas ou meios externos da CashWay.
- iii. Aos Colaboradores, sem autorização prévia, é vetado emitir opiniões em nome da CashWay ou utilizar informações privadas da CashWay em: e-mails, sites, redes sociais, publicações impressas, fóruns de discussão, serviços da Internet e outros ambientes públicos, em face da possibilidade de divulgação inadvertida.
- iv. O uso da marca, nome ou citação da CashWay deve cumprir os requisitos de autorização por direito de imagem e propriedade.
- v. Os colaboradores são responsáveis por manter as informações da CashWay em locais seguros. Isso se aplica a informações impressas, escritas em quadros ou em outras mídias físicas, que não devem ser deixadas desprotegidas em salas de reuniões, mesas ou qualquer local dentro e fora da empresa.
- vi. O descarte de informações internas, restritas ou confidenciais, contidas em qualquer meio, quer seja impresso, eletrônico, magnético, ou sob qualquer outra forma, deve ser feito de forma segura, garantindo a destruição dos dados de forma que não possam ser novamente recuperados.
- vii. O uso de recursos tecnológicos para gravação, foto e filmagem de qualquer reunião ou evento corporativo não é permitido sem prévia autorização e consentimento de todos os participantes.

### **3.12. Conformidade**

- i. O cumprimento e aderência às leis, regulamentações, Política de Segurança Cibernética e da Informação, normas, obrigações contratuais, e padrões de segurança, são obrigatórios e devem ser garantidos por todos os Colaboradores da CashWay
- ii. Responsáveis por recursos críticos da CashWay devem garantir a retenção de evidências da execução de seus controles para fornecimento em casos de auditorias ou necessidade do atendimento a regulamentações.

### **3.13. Conscientização e Divulgação de Segurança Cibernética e da Informação**

- i. A Política de Segurança Cibernética e da Informação, normas e padrões de segurança devem ser amplamente divulgadas no processo de admissão e integração de novos Colaboradores, tanto pela equipe de Recursos Humanos quanto pelos Gestores.

- ii. Programas de conscientização, divulgação e reciclagem do conhecimento da Política de Segurança Cibernética e da Informação devem ser estabelecidos e praticados regularmente para garantir que todos os Colaboradores e terceiros conheçam as diretrizes e responsabilidades relacionadas à segurança das informações.

### **3.14. Continuidade de Negócios**

Deve-se estabelecer, documentar, implantar e manter processos, procedimentos e controles para assegurar o nível requerido de continuidade para os serviços e processos de negócio da CashWay, durante situações adversas. O modelo a ser adotado para a Gestão de Continuidade de Negócios deverá ser baseado na Norma ISO 22301.

### **3.15. Segurança Física**

- i. Os equipamentos e instalações de processamento de informação críticas ou sensíveis, bem como as próprias informações sensíveis, deverão ser mantidos em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.
- ii. As áreas seguras da CashWay devem ser protegidas por controles apropriados de entrada para assegurar que somente pessoas autorizadas tenham acesso.
- iii. O acesso de qualquer pessoa às instalações da CashWay somente deverá ser feito mediante autorização por Colaboradores responsáveis por esse controle e mediante identificação do visitante.
- iv. Nenhum visitante tem a autorização de circular pelas dependências da CashWay sem estar acompanhado por um colaborador CashWay.
- v. As recepções e áreas de maior criticidade devem estar sob proteção de um circuito interno de câmeras de vídeo, instaladas em locais estratégicos. As imagens obtidas devem ser preservadas com segurança.

### **3.16. Acesso Lógico**

- vi. O processo de gestão dos acessos a qualquer sistema da CashWay quer seja interno ou em nuvem, deve ser conduzido pela área de TI, exceções deverão ser tratadas junto a alta direção.
- vii. O acesso a qualquer sistema tecnológico da CashWay deve ser autenticado, ou seja, protegido por credenciais de acesso, certificados, *tokens* ou qualquer outro método seguro de identificação e autenticação.

- viii. Acessos a informações e a sistemas da CashWay devem ser permitidos apenas após dois ou mais níveis de autorização, sendo o primeiro do gestor do colaborador solicitante e o segundo do responsável pela informação ou sistema.
- ix. Os acessos de colaboradores e terceiros devem ser desativados assim que desligados ou encerrados contratos de prestação de serviços.
- x. As credenciais de acesso a sistemas e informações, compostas por usuário e senha, são concedidas pela CashWay aos Colaboradores e Terceiros para uso em atividades relacionadas a seu trabalho, pelo tempo em que perdurar seu vínculo com a empresa.
- xi. É proibido transferir, compartilhar, emprestar ou revelar a senha das credenciais de acesso concedidas pela empresa a outros colaboradores, assim como é proibido o uso de credenciais de outros colaboradores.
- xii. Todos os perfis de usuários e acessos a informações ou sistemas de média e alta criticidade devem ser revisados periodicamente pelo respectivo responsável, seguindo os critérios de segregação da função e observando o princípio de mínimo acesso (*least privilege*) e necessidade de conhecimento (*need to know*).

### **3.17. Gestão de risco de Segurança da Informação**

- i. A Gestão de Riscos de Segurança da Informação deve ser realizada através de um processo estruturado que contemple a identificação, análise, avaliação, priorização, comunicação, tratamento e monitoração dos riscos que podem afetar negativamente os negócios da organização.
- ii. O processo de gestão de riscos deve contemplar novos ativos, sistemas ou processos, quer sejam eles internos, em nuvem ou conduzidos por parceiros.

### **3.18. Incidentes de Segurança da Informação**

- i. São considerados incidentes de segurança da informação quaisquer eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de SI: confidencialidade, integridade, disponibilidade e conformidade, colocando o negócio em risco.
- ii. Violações ou tentativas de violação desta Política, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.
- iii. Colaboradores devem informar imediatamente à segurança da informação todas as violações à Política de segurança da informação, normas, padrões incidentes ou anomalias que possam indicar a possibilidade de incidentes, sobre os quais venham a tomar conhecimento.

- iv. A identificação de incidentes de segurança pode ocasionar o bloqueio imediato dos acessos dos colaboradores envolvidos até que sejam concluídas as investigações necessárias.

### **3.19. Monitoração**

- i. Todas as ações de colaboradores e visitantes, realizadas nas dependências da CashWay ou remotamente, abrangendo o acesso físico e a utilização de recursos de tecnologia da informação e comunicação do grupo, podem ser monitoradas.
- ii. A área de TI é responsável por garantir a privacidade dos registros oriundos da monitoração do acesso e uso de sistemas e serviços de Tecnologia da Informação.
- iii. Ao acessarem sistemas e recursos tecnológicos da CashWay, Colaboradores e visitantes concordam que suas ações podem ser monitoradas.
- iv. Os registros obtidos através de monitoramento poderão ser utilizados em processos de investigação de incidentes e suspeitas de violação de leis e de Normas do Grupo, bem como, em processos judiciais e trabalhistas, a critério da CashWay.

### **3.20. Privacidade**

- i. Deve-se assegurar a privacidade e a proteção, conforme previsto pela legislação e regulamentação pertinente, todas as informações pessoais de clientes, colaboradores, parceiros de negócio e outras que venham a ser armazenadas, processadas ou colocadas sob custódia da CashWay.

### **3.21. Propriedade Intelectual**

- i. A CashWay é proprietária ou custodiante responsável por toda a informação criada, armazenada, transmitida, transportada, processada ou descartada pelos seus recursos ou por aqueles contratados pela CashWay em nuvem ou prestados por terceiros devidamente autorizados.
- ii. É vetada aos Colaboradores a violação da propriedade intelectual do grupo ou de terceiros, quer seja por meio da utilização indevida de imagens, textos, softwares, marcas ou pela cópia indevida de originais ou conversão do formato destes.

### **3.22. Utilização de Recursos de Tecnologia da Informação**

- i. Para utilização de qualquer recurso de tecnologia da informação é necessária à aprovação prévia do gestor do colaborador/terceiro e do proprietário da informação, sistema ou recurso.

- ii. Não é permitida aos Colaboradores e Terceiros a instalação de qualquer software ou a alteração de parâmetros de configuração de computadores da CashWay. Estas devem ser realizadas por equipes de TI autorizadas, após processos de homologação e obtenção do licenciamento adequado. Softwares instalados indevidamente poderão ser automaticamente excluídos, sem prévio aviso.
- iii. É proibido o armazenamento, transmissão, processamento e impressão de conteúdo que contenha pedofilia, pornografia, erotismo, violência, terrorismo, racismo, intolerância, e outros conteúdos proibidos por leis, moral, ética e normas da CashWay.
- iv. As informações internas, restritas e confidenciais ou sensíveis da CashWay não devem ser copiadas, sincronizadas ou replicadas em serviços em nuvem, exceto situações analisadas e aprovadas pela alta direção.
- v. Informações da CashWay ou sob sua custódia e responsabilidade, somente podem ser transportadas ou processadas em meios previamente aprovados pela alta direção, a exemplo e-mail pessoal, Internet, pendrive, redes sociais, CD/DVD, papel, computador pessoal dentre outros meios.
- vi. O acesso de celulares, smartphones, tablets e qualquer outro dispositivo a serviços e informações da CashWay deve ser permitido apenas após o atendimento integral dos requisitos de segurança da CashWay definidos nas normas para esta categoria de dispositivos.
- vii. Documentos eletrônicos de uso da CashWay devem ser armazenados em repositórios centralizados da rede (servidores de arquivos) com as devidas proteções de segurança, dentre elas: controle de acesso e backup. Documentos eletrônicos do grupo não devem ser armazenados em estações de trabalho.
- viii. Os colaboradores devem zelar pela segurança de ativos da empresa colocados sob sua responsabilidade, como dispositivos móveis e notebooks.
- ix. O uso de recursos de criptografia deve ser autorizado pela área de TI e estar de acordo com os padrões definidos para a CashWay.

### **3.23. Segurança em Redes**

- i. Devem existir controles tecnológicos para proteger o acesso entre redes (incluindo Internet, redes públicas, extranets, acesso remoto, wireless e as diferentes redes de usuários).
- ii. Equipamentos com diferentes requerimentos de segurança devem ser segregados em redes diferentes.
- iii. Além do controle de acesso entre as redes, deve ser protegida a informação em trânsito, seguindo os requerimentos da Classificação da Informação.

- iv. O acesso remoto somente será permitido para situações em que for indispensável e esteja documentado e com mecanismos de autenticação de dois fatores.
- v. Os níveis de segurança (confidencialidade, integridade e disponibilidade) esperados dos serviços de comunicações, devem ser estabelecidos nos contratos firmados com os fornecedores desses serviços.
- vi. Deve ser implementado controle tecnológico de *Firewall* para a proteção das redes mais críticas.
- vii. Controles criptográficos devem ser solicitados, estabelecidos e/ou desenvolvidos, para garantir os níveis de confidencialidade das informações trafegadas, segundo a sua classificação (definido pelo proprietário da informação).

#### **3.24. Registros de Auditoria**

- i. Todas as ações de usuários, sistemas e qualquer evento de Segurança da Informação devem gerar trilhas de auditoria (logs), que deverão ser mantidos por um período mínimo de 5 anos, em local centralizado e protegido contra acessos não autorizados.
- ii. Não deve haver nenhuma modificação na integridade das trilhas de auditoria (logs), ou seja, não pode haver usuários com permissão de alteração.
- iii. Todo acesso de consulta, cópia ou tentativa de modificação e exclusão as trilhas de auditoria (logs) devem ser registradas.
- iv. As falhas nos registros das trilhas de auditoria (logs) devem ser registradas, analisadas e devem ser tomadas providências para corrigir o erro de forma imediata.

#### **3.25. Backups, arquivamento e restaurações**

- i. A área de TI deve determinar os recursos requeridos para cumprir com os requerimentos mínimos de respaldo dos ativos de informação, conforme definido pelos proprietários da informação.
- ii. A área de TI deverá estabelecer um plano de backup para cumprir com esses requisitos e deverá estabelecer mecanismos para a correta execução das rotinas de backup.
- iii. Diariamente devem ser validados os resultados da realização dos backups, sendo que as falhas deverão ser reportadas como incidente de segurança.
- iv. O processo de backup e restauração para todos os sistemas deve ser testados em intervalos regulares, com o objetivo de assegurar que estejam em conformidade com os requerimentos dos donos da informação e com as exigências do plano de continuidade do negócio da companhia.

- v. O tempo necessário que a informação deve ser mantida deverá estar de acordo com as necessidades do negócio e deve levar em consideração as exigências das leis vigentes.

### **3.26. Análise de Vulnerabilidades Técnicas**

- i. Periodicamente devem ser realizados testes de vulnerabilidades técnicas dos equipamentos críticos da infraestrutura.
- ii. Após os levantamentos, as comparações e identificações dos riscos devem ser executadas, possibilitando o tratamento dos riscos de acordo com seus níveis.
- iii. Nos casos em que não for possível a eliminação total da vulnerabilidade, deve ser apresentada aceitação do risco ou a determinação de falso positivo.
- iv. Verificações ou auditorias regulares devem verificar a conformidade com as exigências técnicas dos sistemas e das redes.
- v. As auditorias realizadas por terceiros devem identificar claramente as interações com os sistemas em operação.
- vi. As auditorias técnicas dos sistemas e das redes devem respeitar as práticas estabelecidas e devem ser realizadas de acordo com as recomendações da organização. Estas auditorias devem ser realizadas por fornecedores reconhecidos e competentes.

### **3.27. Prevenção, Detecção de Intrusão**

- i. Todos os recursos do sistema de informação expostos à Internet devem ser acompanhados e protegidos por um IDS / IPS.
- ii. Sempre que o IDS / IPS detecta ou responde a uma tentativa externa mal-intencionada suficientemente grave para ameaçar os recursos do sistema de informações protegidas, uma análise estruturada e procedimento de resposta deve ser acionado.

### **3.28. Proteção contra códigos maliciosos**

- i. Deverão ser implementados controles tecnológicos para a proteção dos equipamentos de processamento de informação que executem algum tipo de software (tanto de usuário final como servidores) para a prevenção, detecção, correção e erradicação de códigos executáveis maliciosos.
- ii. Deve ser verificada a atualização das ferramentas de proteção baseadas em assinaturas, para que estejam nas últimas atualizações disponíveis.

### **3.29. Troca de Informações**

- i. A transmissão digital de informações através de canais de comunicação não-seguros deve ser protegida de acordo com o nível da classificação da informação, especialmente analisando a necessidade de utilização de criptografia para a proteção da informação.
- ii. A transmissão física de informações digitais deve ser protegida segundo a classificação da informação. Rótulos, lacres, assinaturas e criptografia devem ser considerados.
- iii. O estabelecimento de comunicações entre redes protegidas com parceiros (Extranets) deve ser protegido por mecanismos criptográficos, ou outros mecanismos similares para proteger a confidencialidade e integridade da informação.
- iv. As áreas de negócio devem sempre utilizar os canais de comunicação seguro (STCP, VPN, SSH, etc.) para envio e recebimento de informações confidenciais entre parceiros e fornecedores, quando possível. Quando não for possível utilizar esse canal a informação deve ser protegida com criptografia ou senha forte, para evitar vazamento das informações.

### **3.30. Controles Criptográficos**

- i. Deverão ser utilizados controles criptográficos para proteger as informações segundo os requerimentos da sua classificação.
- ii. Somente algoritmos de criptografia aprovados pela área de TI podem ser utilizados nas soluções e sistemas adotados pela CashWay.
- iii. O gerenciamento das chaves de criptografia deve prever mecanismos para o armazenamento seguro, geração segura da chave e destruição da chave.
- iv. Deverá existir um mecanismo de recuperação da informação caso seja perdida uma chave de criptografia.
- v. As chaves de criptografia devem ser trocadas periodicamente, dependendo da sua frequência de utilização.
- vi. Caso seja comprometida uma chave criptográfica, deve ser revogada imediatamente. Se for uma chave para criptografia de arquivos, deve ser trocada.
- vii. Mecanismos de autenticação e auditoria devem ser estabelecidos para garantir a segurança do acesso às chaves.

### **3.31. Aquisição, Desenvolvimento e Manutenção Segura de Sistemas**

- i. Sistemas da informação desenvolvidos ou adquiridos devem contar com atributos e funcionalidades de segurança que protejam adequadamente as informações. Os requerimentos devem ser identificados e documentados na fase de concepção do sistema, para assegurar que as demandas de segurança sejam atendidas.

- ii. Deve haver controles que previnam erros de operação, perda, ou vazamento de informações. Todo sistema deve ser documentado, tornando sua implantação e operação independente de conhecimentos informais.
- iii. Devem ser estabelecidos controles criptográficos para proteger a confidencialidade, autenticidade ou integridade das informações. Faz-se necessária a documentação do uso de chaves, quando necessário.
- iv. Sistemas devem ser protegidos contra alteração indevida, evitando a exposição de dados sensíveis. Devem ser estabelecidos controles para monitorar e corrigir as vulnerabilidades e falhas desses.
- v. O acesso ao código fonte das aplicações deve ser protegido, seguindo as características definidas pela classificação da informação.
- vi. Somente colaboradores autorizados devem ter acesso ao código-fonte, com os correspondentes controles de versão.
- vii. As instalações de desenvolvimento, teste e produção devem ser separadas. Deve haver segregação entre estes ambientes para evitar que dados de um ambiente sejam utilizados em outro.
- viii. Dados reais de produção não serão utilizados para testar aplicativos.
- ix. Dados privados de usuários não serão utilizados para testar aplicativos.
- x. Deverá ser assinado um termo de confidencialidade assim como assinadas as políticas de segurança por parte de terceiros que façam desenvolvimento de sistemas para a CashWay.
- xi. O desenvolvimento de sistemas por parte de terceiros deverá ser controlado e auditado por pessoal técnico da CashWay.
- xii. O desenvolvimento de sistemas deverá seguir as boas práticas de mercado quanto ao Desenvolvimento Seguro.
- xiii. Toda manutenção em sistemas deve:
  - a. Considerar os requerimentos de segurança antes, durante e depois da manutenção;
  - b. Garantir a integridade e a conformidade das especificações funcionais iniciais;
  - c. Respeitar a consistência e a homogeneidade do nível de segurança estabelecido inicialmente no desenvolvimento da aplicação;
  - d. Respeitar, ao efetuar as modificações, os resultados da análise inicial do risco realizada na fase de projeto;
  - e. Garantir a origem e a integridade das entregas para o ambiente de produção;
  - f. Preservar a confidencialidade dos contextos operacionais;

- g. Preservar a segurança dos sistemas ou da rede, assegurando que nenhuma intervenção forneça a oportunidade de sabotagens de forma inesperada ou de ações maliciosas;
- h. Respeitar as obrigações legais e contratuais com relação à confidencialidade das informações processadas pelos sistemas.

### **3.32. Serviço de Nuvem**

- i. A possibilidade de utilização de uma solução de hospedagem externa, e, mais especificamente, uma solução '*cloud computing*', depende do nível de sensibilidade dos dados e os processos em questão. Esta escolha deve ser feita com base em uma análise de risco.
- ii. Toda e qualquer contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deverá ser previamente comunicada ao Banco Central do Brasil.
- iii. Os serviços para processamentos de dados e ou armazenamento em nuvem, sejam eles *software* como serviço (SaaS) ou armazenamento de base de dados devem possuir acesso seguro através de interfaces HTTPS bem como a autenticação segura e em ambientes segregados.
- iv. Os acessos devem ser controlados por meio de logins e senhas individuais, previamente fornecidos, de acordo com a atividade de cada colaborador/terceiro ou administrador, possuindo também tais acessos e ações registrados em trilhas de auditorias.

### **3.33. Gestão de Incidentes de Segurança**

- i. Qualquer evento relacionado a um suposto ou comprovado ataque a segurança de um sistema operacional deve ser resolvido de acordo com um processo de gerenciamento de incidentes.
- ii. Os procedimentos envolvidos devem descrever o processo de gerenciamento de incidente, o processo de investigação e o processo de recolhimento de provas. O processo de gerenciamento de incidente deve:
  - a. Permitir a detecção, o mais cedo possível, e a capacidade de responder com a máxima eficácia para limitar os danos causados pelo incidente;
  - b. Limitar as zonas de vulnerabilidade pela remediação de anomalias identificadas em algum ou todos os sistemas operacionais potencialmente afetados;
  - c. Reter informações relevantes para posteriores investigações e coleta de provas;
  - d. Compilar um registro de incidentes de segurança e estatísticas para uso na previsão de possíveis incidentes futuros;
  - e. Identificar pontos de contato apropriados para o nível de severidade do ataque

- iii. Uma vez que um incidente mal-intencionado for resolvido, uma análise deve ser feita para identificar a origem do ataque e iniciar procedimentos administrativos ou judiciais apropriados.

### **3.34. Gestão de Fornecedores**

- i. O gerenciamento de fornecedores deverá considerar a avaliação de risco e classificação dos fornecedores (estratégico, tático, operacional).
- ii. A intervalos regulares o desempenho dos fornecedores críticos deve ser medido quanto ao cumprimento das metas acordadas e os resultados avaliados. Os resultados devem ser discutidos com o fornecedor para se identificar as necessidades e oportunidades de melhoria.
- iii. Cada fornecedor deverá ter um gestor designado que acompanha o seu desempenho, tornando-o responsável pela qualidade dos serviços fornecidos.

### **3.35. Atualizações desta e demais políticas**

- i. Esta Política está sujeita a revisões anuais, podendo ser revisada em periodicidade menor, caso necessário, em decorrência de alterações na regulamentação e/ou legislação aplicável ou, ainda, para refletir alterações nos procedimentos internos da organização.
- ii. Esta e demais políticas passarão pelo seguinte procedimento de elaboração e revisão:
  - Gestor responsável pela alteração solicitada e/ou inclusão de novo procedimento na política;
  - Avaliação e aprovação do Diretor responsável por esta Política.
- iii. A versão atualizada desta Política será publicada na Internet e Intranet e deverá ser lida por todos os colaboradores.

### **3.36. Aplicabilidade**

- i. O Gestor imediato ou a alta direção devem ser consultados sempre que existir alguma dúvida referente à aplicabilidade da Política de Segurança Cibernética e da Informação e demais documentos que a compõe.
- ii. Cabe à área de TI avaliar os riscos de ações não previstas na Política de Segurança Cibernética e da Informação, se necessário levando o assunto a alta direção.
- iii. Exceções às diretrizes contidas neste documento e nos demais que compõem a Política de Segurança Cibernética e da Informação devem ser autorizadas pela alta direção.

### **4.16. Responsabilidades**

Todo Colaborador, independente do cargo, função ou local de trabalho, é responsável pela segurança das informações da CashWay e deve cumprir as determinações da Política, normas e

padrões de segurança da informação.

**i. Alta Direção**

- Prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação.
- Prover comprometimento e apoio à aderência a Política de Segurança Cibernética e da Informação de acordo com os objetivos e estratégias de negócio estabelecidas para organização;
- Fornecer à área responsável pela Segurança da Informação claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário.
- Identificar requisitos legais pertinentes à segurança da informação;
- Garantir a adoção de cláusulas pertinente à segurança das informações nos contratos estabelecidos com a CashWay.

**ii. Colaborador**

- Utilizar de modo seguro, responsável, moral e ético, todos os serviços e sistemas de TI;
- Notificar a área de TI sobre as violações da Política de Segurança Cibernética e da Informação e sobre os incidentes de segurança que venha a tomar conhecimento;
- Manter o sigilo das informações que tenha obtido acesso enquanto Colaborador da CashWay, mesmo após seu desligamento da empresa.

**iii. Gestor**

- Apoiar e incentivar o estabelecimento da Política de Segurança Cibernética e da Informação na CashWay;
- Garantir que seus subordinados tenham acesso e conhecimento desta Política e demais normas e padrões de segurança da informação;
- Fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança das informações da CashWay;
- Avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;
- Designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;
- Acionar as áreas competentes para a aplicação das penalidades, cabíveis aos Colaboradores que violarem a Política de Segurança Cibernética e da Informação e as normas da CashWay;
- Autorizar acessos de seus colaboradores apenas quando forem realmente necessários e segundo os conceitos de *need to know* e *least privilege*.

**iv. Área de Infraestrutura**

- Orientar e coordenar as ações de segurança da informação, promovendo a execução de acordo com o que foi estabelecido;
- Desenvolver e estabelecer programas de conscientização e divulgação da Política de Segurança Cibernética e da Informação;
- Conduzir o processo de Gestão de Riscos de Segurança da Informação;
- Conduzir a Gestão de Incidentes de Segurança da Informação, incluindo as investigações para determinação de causas e responsáveis e a comunicação dos fatos ocorridos;
- Conduzir os processos de monitoração e segurança da informação;
- Definir controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de SI;
- Propor projetos e iniciativas para melhoria do nível de segurança das informações da CashWay.
- Manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de hardware e software;
- Tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia;
- Conduzir a gestão dos acessos a sistemas e informações da CashWay;
- Implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;
- Informar imediatamente a alta direção, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos da CashWay;
- Controlar alterações em ativos de TI e garantir que estas sejam analisadas criticamente e testadas para que não ocorram impactos adversos na operação da empresa ou em sua segurança;
- Garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio.
- Garantir que todos os ativos críticos de Tecnologia da Informação devem ser instalados em ambientes especializados conhecidos como Datacenters. Estes devem conter todas as proteções e contingências necessárias para a sua respectiva proteção.
- Monitorar o acesso físico de Colaboradores às instalações do GPA;
- Administrar o controle de acesso físico.

#### **v. Recursos Humanos**

- Verificar o histórico de candidatos a emprego, de acordo com a ética e leis vigentes;
- Garantir que a Política, Normas e Procedimentos da Política de Segurança Cibernética e da Informação sejam divulgados no processo de admissão/integração de novos Colaboradores.

#### **vi. Fornecedores e Parceiros de Negócios**

- Cumprir as determinações da Política, Normas e Procedimentos publicados pela CashWay;
- Orientar os funcionários da empresa sobre o cumprimento das determinações da Política, Normas e Procedimentos publicados pela CashWay;
- Cumprir com o acordo de confidencialidade.

#### **4. PENALIDADES**

O Colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração ao Gerente de Infraestrutura. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

#### **Observação**

No caso de Colaboradores terceiros, pode ser solicitada às suas respectivas empresas a troca da equipe alocada na CashWay, ou ainda, podem ser aplicadas penalidades a empresa tais como, multas, cancelamento do contrato e ações judiciais.

#### **5. ANEXOS**

Não se aplica.

#### **6. REFERÊNCIAS**

- Norma ISO/IEC 27001 e 27002;

**CASHWAY TECNOLOGIA DA INFORMAÇÃO S.A.**