



Versão: 1.0 –
Documento Integrado Órgão
Aprovador: Diretoria Executiva e
Conselho de Administração

Vigência: A partir da data de
aprovação 11/11/2025 Revisão
mínima: Anual ou sempre que
houver alteração regulatória
relevante

Política de Segurança da Informação da BRASCARD

As diretrizes de Segurança da Informação e Cibernética da BRASCARD aderem-se integralmente ao comprometimento da alta administração e aos objetivos estratégicos dos negócios da organização e assegura o cumprimento das exigências normativas, de órgãos reguladores, de Compliance e requisitos legais de todo o ambiente da BRASCARD.

A BRASCARD trabalha com princípios que visam garantir a proteção da informação de nossos clientes, parceiros, terceiros, profissionais ou qualquer instituição ou pessoa que tenha relacionamento com a companhia, são eles:

Confidencialidade

Somente o usuário da informação, que esteja devidamente autorizado pelo Gestor da Informação, deve ter acesso às Informações respeitando os critérios de segregação de funções pré-definidos;

Integridade

Garante que informações não sejam alteradas desde a sua criação até seu uso. Eventuais alterações, supressões e/ou adições devem ser autorizadas pelo Gestor da Informação;

Disponibilidade

Procura garantir que as Informações estejam sempre disponíveis para o Usuário da Informação;

Autenticidade

Garante a identidade de quem está enviando a Informação;

Esses pilares são a base para que os processos de Governança da Segurança da Informação e Cibernética sejam atendidos e controlados, de forma a:

Estabelecer diretrizes para a classificação de dados e informações, por meio de critérios e restrições para acesso, processamento ou transmissão da informação confidencial, sensível ou restrita da BRASCARD, parceiros ou de seus clientes que não tenham sido autorizadas pelos responsáveis;



Versão: 1.0 –
Documento Integrado Órgão
Aprovador: Diretoria Executiva e
Conselho de Administração

Vigência: A partir da data de
aprovação 11/11/2025 Revisão
mínima: Anual ou sempre que
houver alteração regulatória
relevante

Implementar procedimentos e controles para mitigação das vulnerabilidades, incidentes e riscos de segurança, sinalizar a saúde do ambiente e produzir planos de remediação e/ou contenção, geração de riscos de segurança, além de informações sobre a situação e estado dos ativos frente as preocupações, ameaças de acordo ao apetite à risco e às estratégias das Companhias, reduzindo assim as superfícies de ataques e os respectivos riscos associados;

Realizar a gestão, identificação, resposta, tratamento e redução de incidentes de segurança da informação, assim como o monitoramento proativo, a detecção e a investigação de tais ocorrências, por meio dos serviços de inteligência (threat intelligence) e ainda, comunicar e/ou compartilhar (quando aplicável e especialmente no caso de incidente relevante) as áreas envolvidas, os órgãos reguladores, parceiros de inteligência e entidades externas;

Prover mecanismos de prevenção ao vazamento de dados e informações (Data Loss Prevention – DLP), para detecção de possíveis violações ou padrões de condutas que possam infringir regulamentos das Companhias;

Disponibilizar mecanismos de proteção, por meio do monitoramento de atividades de endpoints, sensores e controles de proteção de hardware ou software, contra códigos maliciosos que uma vez executados possam se infiltrar ou causar danos nas redes ou ativos das Companhias;

Prover diretrizes de utilização dos recursos de rede, ou em contexto mais abrangente, dos recursos computacionais, sejam estes ativos fixos e/ou dispositivos móveis, removíveis, visando as melhores práticas de manipulação, proteção, processamento, monitoração e compartilhamento de informações;

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA Áreas responsáveis:
Segurança da Informação & Compliance Data: NOVEMBRO DE 2025

Prover planos e subplanos (Impacto no Negócio, Continuidade Operacional, Recuperação de Negócios, Gerenciamento de Incidentes, Administração de Crises e Planos de Testes/Validações) de recuperação de serviços críticos para garantir a disponibilidade operacional e da continuidade de negócio, bem como, procedimentos operacionais que possam reduzir os impactos decorrentes da interrupção de serviços causada por desastres, crises, indisponibilidades, falhas, comprometimentos ou eventos relevantes de segurança;



Versão: 1.0 –
Documento Integrado Órgão
Aprovador: Diretoria Executiva e
Conselho de Administração

Vigência: A partir da data de
aprovação 11/11/2025 Revisão
mínima: Anual ou sempre que
houver alteração regulatória
relevante

Gerenciar e monitorar via Controle de Acessos, sejam estes físicos e/ou lógicos, às informações e ativos bem como o seu armazenamento, compartilhamento e descarte, para que somente pessoas autorizadas possam utilizá-los e em conformidade com regras, permissões, perfis e/ou políticas corporativas;

Estabelecer critérios seguros de uso e manutenção de credenciais, segredos, tokens e senhas no contexto de utilização dos sistemas corporativos;

Dar ciência aos profissionais, usuários, prestadores de serviços, clientes e parceiros de que: o não é permitido remover controles de segurança ou aplicações utilizadas para o acesso das informações ou proteção, bem como prover alterações em ambiente produtivo sem prévia aprovação; os meios de comunicação, equipamentos de acesso a sistemas de informações e infraestruturas complementares são de propriedade da Companhia e passíveis de monitoração, sendo que os acessos ao conteúdo da internet e uso de e-mail é de responsabilidade do profissional titular da conta, do prestador de serviço, cliente ou parceiro, estando sujeito à aplicação de leis, decretos e regulamentos governamentais vigentes; e o não é permitido o uso de qualquer recurso tecnológico ou informações proprietárias em ações ilegais e nem a instalação de recurso computacional não autorizado.

Definir controles fundamentais para o ciclo de vida e desenvolvimento seguro de software, utilização de novas tecnologias que possam guiar projetos dentro do contexto software seguro;

Ajudar no dimensionamento dos requisitos de segurança a partir de arquitetura de referência, uso de controles criptográficos e proteções necessárias de acordo com a complexidade e nível de segurança necessário para cada componente;

Garantir que sistemas desenvolvidos internamente ou adquiridos de fornecedores atendam aos padrões de segurança e melhores-práticas definidos pelo mercado ou pelas necessidades de negócio;

Estabelecer diretrizes para manutenção de cópias de segurança (backup e restore) de dados e informações para os repositórios e locais de armazenamento oficiais das Companhias, assim como regimentos para a retenção da informação e logging, em conformidade com os órgãos reguladores e questões legais vigentes;

Divulgar continuamente em todos os níveis, esferas e para o maior público possível, interna e/ou externamente (aos clientes) quando aplicável, programas e ações de conscientização,



Versão: 1.0 –
Documento Integrado Órgão
Aprovador: Diretoria Executiva e
Conselho de Administração

Vigência: A partir da data de
aprovação 11/11/2025 Revisão
mínima: Anual ou sempre que
houver alteração regulatória
relevante

treinamentos, acultramento e prevenção em relação à temática de Segurança da Informação e Cibernética;

Analisar, aprovar e classificar contratos, nos termos da legislação vigente e sob o POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA;

Suportar questões de risco oferecendo um modelo e processo de risco comum, integrado e contínuo de identificação, análise, avaliação, tratamento, revisão e comunicação dos riscos mapeados, a fim de proteger os ativos das companhias em avaliações e definições de controles que possam validar o escopo desta política no intuito de aferir o nível de segurança dos controles de segurança da informação, em atendimento às áreas demandantes (Auditoria Interna, Controles Internos e Compliance). A violação de controle de segurança ou o não cumprimento das diretrizes é considerada infração e poderá implicar em medidas disciplinares (sanções) a serem validadas pelos departamentos de Recursos Humanos, Jurídico, Compliance e Segurança da Informação BRASCARD, conforme sua natureza e enquadramentos previstos nas leis vigentes.