POLÍTICA DE RISCOS CIBERNÉTICOS
PORTO SEGURO S.A

1. OBJETIVO

A Porto estabelece neste documento as diretrizes e requisitos de riscos cibernéticos para compor a proteção dos ativos tecnológicos, processos e pessoas que interagem no ambiente do Grupo Porto, visando a confidencialidade, integridade e disponibilidade dos dados.

2. ABRANGÊNCIA

Esta Política se aplica a todos os colaboradores, prestadores de serviço e qualquer pessoa com poderes de representação da Porto Seguro S.A. e suas controladas direta ou indiretamente.

3. REFERÊNCIAS NORMATIVAS

Servem de referência para os procedimentos descritos neste documento, os seguintes normativos:

- Lei nº 13.709/18 - Lei Geral de Proteção de Dados;
- Circular SUSEP Nº 638, de 27 de julho de 2021;
- Resolução CMN 4.893/21 Banco Central do Brasil;
- NIST CSF - Cyber Security Framework;
- ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação;
- ISO/IEC 27002 – Código de prática para controles de segurança da informação;
- ISO/IEC 27005 – Gestão de riscos de segurança da informação;
- ISO/IEC 27701 – Sistema de Gestão de Privacidade;
- ISO/IEC 22301 – Sistema de Continuidade de Negócios;

4. DEFINIÇÃO DE RISCOS CIBERNÉTICOS

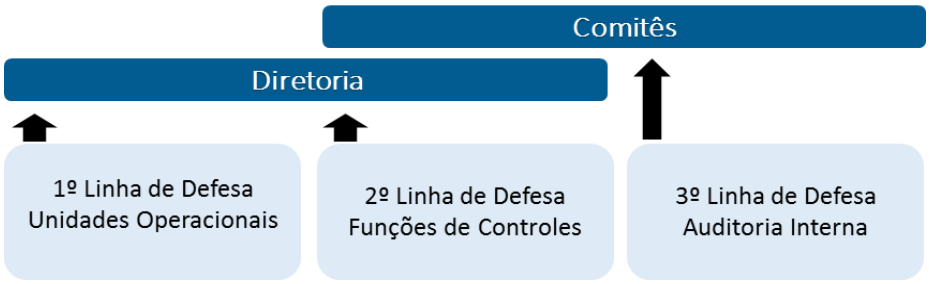
Riscos cibernéticos na Porto é definido como o risco de perda financeira, interrupção da comunicação ou dano à reputação do Grupo decorrente da exposição de dados, processos, pessoas e tecnologias a ameaças digitais.

5. MISSÃO DE RISCOS CIBERNÉTICOS

Identificar e direcionar os riscos cibernéticos e as ameaças digitais que possam comprometer a confidencialidade dos dados, a integridade, reputação da marca, resultados financeiros e estratégias da Porto.

6. ESTRUTURA DE GERENCIAMENTO DE RISCOS CIBERNÉTICOS

A abordagem de três linhas de defesa é a base da estrutura de gestão de riscos da Porto, onde temos:



Primeira linha de defesa (Unidades Operacionais) – As Diretorias Executivas e suas unidades operacionais, tais como, tecnologia da informação e segurança da informação, têm responsabilidade primária pelos riscos que decorrem de sua atividade. Desta forma é esperado que estas unidades adotem procedimentos e controles adequados para que a gestão esteja alinhada com as diretrizes definidas pela organização.

Segunda linha de defesa (Funções de Controle) – As funções de controle têm como responsabilidade de orientar e supervisionar se os processos e controles definidos pela primeira linha de defesa estão de acordo com as diretrizes organizacionais. As funções de controle são independentes da operação e estão relacionadas principalmente às áreas de Riscos Cibernéticos (cuja missão é dar visibilidade dos riscos e ameaças cibernéticas que podem comprometer o negócio e que estes riscos sejam efetivamente identificados, mensurados, direcionados, acompanhados e reportados de forma independente), Gestão de Riscos Corporativos, Compliance e Controles Internos.

Terceira linha de defesa (Auditoria Interna) – A função de auditoria interna atua de forma mais ampla e independente na verificação da aderência às diretrizes ao avaliar a eficácia do ambiente de gestão e controle de riscos (supervisão sobre a primeira e segunda linha de defesa).

Conforme descrito acima, a governança de gerenciamento de riscos conta com a participação de todas as áreas, tendo por finalidade proteger o resultado do Grupo e seus acionistas, contribuir para sua sustentabilidade e valor, envolvendo aspectos relacionados à transparência e prestação de contas.

Refletindo o compromisso com o direcionamento dos riscos cibernéticos, o Grupo Porto possui na segunda linha de defesa a Superintendência de Riscos que é composta entre outras estruturas, pela Gerência de Riscos Cibernéticos.

7. PRINCÍPIOS

O Grupo adota princípios que devem orientar o modelo de gerenciamento dos riscos cibernéticos, incluindo:

- Existência de processo formal voltado ao gerenciamento dos riscos cibernéticos, inclusive àquele relacionado a serviços terceirizados, compatível com a natureza e a complexidade dos produtos, serviços, processos, atividades e sistemas computadorizados do Grupo;

- Existência de definição de funções, atribuição de responsabilidades, limites de tolerância a riscos e de delegação de autoridades que subsidiam a administração efetiva dos riscos cibernéticos;

- Realizar, no mínimo anualmente, a revisão da política e do processo de gerenciamento dos riscos cibernéticos;

- Estabelecer e difundir em toda instituição a definição dos riscos cibernéticos, assim como critérios e procedimentos a serem adotados para sua identificação, avaliação, controle, monitoramento, mitigação e reporte tempestivo às alçadas competentes;

- Conscientizar, educar e capacitar os profissionais e parceiros de serviço quanto ao atendimento das políticas de segurança da informação, riscos cibernéticos e instruções normativas correspondentes, visando aderência e cumprimento da governança dos riscos cibernéticos em vigor no Grupo;

- Direcionar o adequado controle e monitoramento dos mecanismos de segurança da informação, visando manter o ambiente tecnológico seguro de ataques cibernéticos, roubo de informações e acessos indevidos, além de manter a integridade dos dados;

- Validar que as atividades sejam monitoradas com eficácia, de forma a permitir, com base em pontos de controles e relatórios quantitativos e qualitativos, a identificação dos processos com impacto, permitindo a implementação de planos de ação preventivos ou mesmo corretivos;

- Realizar periodicamente testes sobre os domínios de prevenção e reação aos riscos cibernéticos, considerando processos, procedimentos, pessoas e tecnologias envolvidas no negócio com apoio na elaboração de planos de ação integrados sobre os cenários de risco identificados;

- Zelar pelo pleno funcionamento do parque tecnológico (servidores, desktops, banco de dados) permitindo o suporte as operações de negócio e a disponibilidade dos produtos e serviços da Porto;

- Assegurar a existência de Planos de Contingência e de Continuidade de Negócios que preservem a capacidade do Grupo em operar e limitar as perdas operacionais decorrentes da interrupção parcial ou total das atividades;

- Assegurar que todas as alterações ou desenvolvimento de novos produtos e sistemas tenham uma avaliação dos riscos cibernéticos a eles vinculados;

- Manter um sistema de classificação das exposições digitais conforme a natureza da operação, ameaça e o risco associado, considerando critérios consistentes e passíveis de verificação;

- A proteção da imagem, marca e valor do Grupo Porto no cenário digital;

- Contemplar em seus processos, procedimentos, tecnologias e rotinas operacionais mecanismos e recursos que preservem a confidencialidade, integridade e disponibilidade das informações, incluindo informações de terceiros que venham a fazer parte das estruturas de tecnologia e negócios do Grupo;

- Prover o acesso as informações de maneira controlada, preservando as necessidades de negócio e a proteção cibernética do Grupo, provendo mecanismos para reduzir a possibilidade de acessos indevidos e alteração não autorizada da integridade das informações.

- Identificar violações de segurança cibernética, estabelecendo processos, procedimentos, normativas, rotinas operacionais, conscientização e tecnologias para detecção de anomalias no ambiente que se caracterizem como comprometimento das barreiras de proteção cibernética do Grupo.

- Estabelecer ações sistêmicas, embasadas por processos, procedimentos e normativas, para resposta de incidentes cibernéticos, identificação e tratativa de vulnerabilidades tecnológicas e de acesso físico em ambiente com informações sensíveis, com o objetivo de direcionar os riscos cibernéticos associados as estratégias de negócio e operações de suporte ao Grupo.

- Atender a legislação em vigor, respeitando a regulamentação dos órgãos reguladores correspondentes e que atendam a proteção do negócio, dos clientes e dos parceiros de serviço no ambiente cibernético da Porto.

8. DIRETRIZES

A seção a seguir apresenta os vinte e dois domínios baseados em normativas ou frameworks como ISO 27001 e NIST, contemplados nas rotinas que visam a gestão dos riscos cibernéticos da Porto e sendo necessário ser seguido pelos colaboradores e terceiros.

Arquitetura técnica de segurança da informação

Estabelece os modelos de referência e componentes tecnológicos de defesa cibernética a serem utilizados em sistemas de informação, com base em sua criticidade para o Grupo Porto.

Gestão de ativos tecnológicos

Estabelece a gestão de ativos físicos e lógicos, considerando não apenas os ativos internos, assim como aqueles que podem ser transitados fora do ambiente tecnológico do Grupo Porto.

Conscientização

Elabora e dissemina o programa de conscientização de Riscos Cibernéticos, considerando não apenas os colaboradores assim como prestadores de serviço ou qualquer pessoa com poderes de representação da Porto Seguro S.A. e suas controladas direta ou indiretamente.

Continuidade de negócios

Estabelece e mantém a capacidade de preservação e continuidade dos negócios considerando o mínimo necessário, ou seja, processos, pessoas, tecnologias e negócios críticos do Grupo que devem ser mantidos em caso de cenário de crise.

Proteção de dados

Estabelece os padrões de proteção de dados de forma a manter a confidencialidade e integridade dos dados do Grupo Porto.

Governança de riscos cibernéticos

Estabelece a gestão dos riscos cibernéticos, afim de minimizar a exposição dos dados da Porto.

Segurança dos hosts

Estabelece as diretrizes gerais de proteção lógica dos ativos tecnológicos da Porto.

Gestão de identidades e acessos

Controla e segrega o acesso a dados e transações, mitigando o excesso de privilégios que possam levar a vazamento de informações, acesso indevido, fraudes ou mesmo ações que impactem a imagem do Grupo.

Resposta a incidentes

Direciona a atuação sobre incidentes cibernéticos na organização e seus mecanismos de resposta e redução do impacto provocado por ações indevidas ou em não conformidade com as políticas e normativos do Grupo.

Métricas e relatórios

Mantem a alta administração do Grupo e líderes de negócios informados quanto a exposição dos negócios a riscos e ameaças cibernéticas que possam comprometer a imagem, operações, saúde financeira, compliance ou a reputação do Grupo assim como de seus colaboradores.

Segurança de redes

Mantém a disponibilidade do ambiente da Porto e a confidencialidade e integridade das informações armazenadas e trafegadas, por meio de um conjunto de controles de segurança da informação.

Operações de segurança da informação

Manutenção e sustentação da operação de segurança da informação, tendo como apoio as diretrizes, políticas e normativas corporativas estabelecidas em linha com as estratégias de negócio da Porto.

Políticas e instruções normativas

Estabelece as diretrizes por meio de políticas e normativas criadas pela Gerência de Riscos Cibernéticos. Com essas diretrizes, é esperado dos profissionais, terceiros e parceiros de serviço comportamento preventivo contra ameaças e riscos cibernéticos, afim de preservar a informação, os dados e a reputação da Porto.

Privacidade

Preserva a privacidade das informações que identifiquem pessoas e caracterizem um indivíduo na organização.

Monitoramento

Prove insumos e medições quanto a possibilidade de desvios de conduta e ações indevidas, de forma a preservar a segurança dos dados de usuários, clientes, e das estratégias de negócio da Porto.

Segurança de software

Preserva a proteção cibernética dos sistemas, aplicativos e aplicações Web da organização, desde suas etapas de desenvolvimento até a manutenção em ambientes de produção.

Estratégia de riscos cibernéticos

Dá ciência a Diretoria e áreas influenciadas sobre o alinhamento de riscos cibernéticos à estratégia de negócio, visão e missão da Porto.

Gestão de riscos cibernéticos de terceiros

Estabelece as diretrizes de segurança no momento da contratação, prevendo as responsabilidades da contratante e do contratado.

Inteligência de ameaças

Mapeia e identifica ameaças cibernéticas que possam comprometer a sustentação da organização, possibilitando ações preventivas através de soluções de segurança integradas de tecnologia, processos, procedimentos e pessoas, minimizando possíveis impactos na Porto antes que impactos possam ocorrer prejudicando a estratégia da organização.

Gestão de vulnerabilidades

Minimiza o risco de exposição cibernética da Porto mediante a identificação e direcionamento sobre as vulnerabilidades tecnológicas mapeadas.

Segurança física

Estabelece diretrizes para a proteção física e de perímetro que protege os dados e informações da Porto.

Segurança em nuvem

Direciona as ações de proteção da informação e de Riscos Cibernéticos da Porto em ambientes e provedores de Nuvem.

9. PAPÉIS E RESPONSABILIDADES

9.1 Conselho de Administração

- Zelar pela perenidade da Companhia, dentro de uma perspectiva de longo prazo e de sustentabilidade, que incorpore considerações de ordem econômica, social, ambiental e de boa governança corporativa, na definição dos negócios e operações;
- Formular diretrizes para a gestão da Companhia e de suas controladas, que serão refletidas no orçamento anual;
- Zelar pela adequação da Estrutura de Gestão de Riscos;
- Aprovar a Política Corporativa de Gestão de Riscos;
- Definir e aprovar o Apetite por Risco e revisá-lo sempre que ocorrer a atualização do plano de negócios.

9.2 Diretoria Executiva

- Avaliar anualmente ou sempre que houver mudança significativa no perfil de risco, a eficácia da Estrutura de Gestão de Riscos Cibernéticos, informando ao Conselho de Administração os resultados dessas análises e as respectivas propostas de ação, caso necessário;
- Acompanhar de forma periódica as informações de riscos cibernéticos aos quais o Grupo esteja exposto;
- Monitorar periodicamente as exposições a risco assim como os planos de ação ou medidas corretivas, caso necessário.

9.3 Comitê de Risco Integrado

- Revisar e validar anualmente a Política de Riscos Cibernéticos;
- Zelar pelo cumprimento das políticas e efetividade do processo de gerenciamento de riscos cibernéticos;
- Prover recomendações relacionadas ao apetite e limites de exposição por tipos de riscos, assim como às Políticas de Riscos Cibernéticos;
- Monitorar o perfil e apetite de risco da Companhia e supervisionar a observância de seus termos;
- Analisar e pontuar fatores de riscos internos e externos que podem impactar os negócios do Grupo Porto;
- Analisar os casos que lhe forem submetidos e sugerir à Diretoria as melhores soluções face às circunstâncias, riscos e custos envolvidos;
- Revisar anualmente o relatório sobre a eficácia das políticas e dos sistemas de gerenciamento de riscos e de controles internos da Companhia.

9.4 Gestores das Unidades Operacionais (Primeira linha de defesa)

- Promover os controles necessários às atividades sob responsabilidade de suas áreas, incluindo o monitoramento dos respectivos riscos;

- Prover condições que assegurem a adequada identificação, classificação, avaliação, mitigação, gerenciamento e reporte dos Riscos Cibernéticos, assim como perdas decorrentes de suas áreas e a efetividade dos controles cibernéticos associados;

- Avaliar os resultados da execução dos testes de controles e estabelecer o encaminhamento de ações voltadas à redução/eliminação de não conformidades, em linha com os prazos associados aos riscos identificados nestas não conformidades;

- Auxiliar a área de Riscos Cibernéticos, provendo acesso às informações necessárias para realização das análises para o desenvolvimento e acompanhamento de limites de riscos;

- Monitorar os serviços terceirizados relevantes para o funcionamento das atividades da Instituição sob sua responsabilidade;

- Apoiar a constituição de grupos de trabalhos, voltados à diagnostico das causas de perdas e à identificação de medidas saneadoras, avaliando e validando os resultados das análises realizadas;

- Propagar a cultura de prevenção a riscos cibernéticos nos times sob sua gestão.

9.5 Segurança da Informação

- Estabelecer processos e controles adequados para preservar a segurança da informação e atendimento das políticas e normativos internos da Porto;

- Atuar para prevenir ou responder a riscos e ameaças cibernéticas conforme as normativas estabelecidas;

- Elaborar e manter procedimentos técnicos de tratamento de incidentes de segurança da informação com apoio das áreas da TI;

- Propor e administrar projetos e iniciativas relacionadas à segurança da informação;

- Estar presente nas áreas de negócio, atuando de maneira preventiva, sobre os riscos e ameaças cibernéticas;

- Gerar métricas e indicadores da exposição da tecnologia a riscos e ameaças cibernéticas.

9.6 Tecnologia da informação

- Atuar de maneira integrada para reduzir a exposição dos negócios a riscos cibernéticos, atendendo as políticas e normativas da Porto;

- Atentar a desvios e rotinas que possam causar a exposição da Porto no cenário cibernético;

- Observar e alertar a área de segurança da informação ou de riscos cibernéticos eventuais desvios de conduta de profissionais ou parceiros de serviço quanto as políticas e normativas da Porto.

9.7 Gestor de Riscos

- Monitorar o perfil de risco e os níveis de exposição, assim como seu alinhamento ao Apetite por Risco.

- Avaliar os processos, metodologias e ferramentas utilizadas para gestão dos riscos, bem como a suficiência e adequação dos recursos humanos e materiais envolvidos nesta atividade nas diversas áreas supervisionadas (1ª linha de defesa);

- Reportar periodicamente e sempre que necessário os resultados dos monitoramentos e análises de risco a Diretorias, Comitê de Risco Integrado (CRI), Comitê de Auditoria e Conselho de Administração;

- Orientar quanto a estratégias e alternativas para gestão de riscos, na medida que isso não comprometa sua independência;

- Participar da análise de mudanças, de forma a auxiliar na avaliação de seus riscos e potenciais implicações/necessidade de alteração na Estrutura de Gestão de Riscos;

- Atuar junto as áreas gestoras em situações de riscos e/ou desenquadramento dos limites, de forma a obter as justificativas e planos de ação necessários;

- Acompanhar a implementação de planos de ação ou medidas corretivas que visem a sanar deficiências da Estrutura de Gestão de Riscos;

- Orientar as unidades operacionais (1ª Linha de Defesa) e Diretoria da Companhia em relação à gestão de riscos;

- Auxiliar as diversas unidades operacionais na identificação/avaliação de seus riscos e consolidar os resultados de forma a garantir sua consistência;

- Propor ações de conscientização dos funcionários da supervisionada em relação aos riscos de suas operações, com o objetivo de reforçar comportamentos e atitudes que favoreçam a gestão dos mesmos;

- Elaborar textos/reportes periódicos referentes a informações de risco a serem divulgadas ao mercado, submetendo-os à validação e aprovação das alçadas competentes.

9.8 Riscos Cibernéticos

- Propor as políticas e instruções normativas de Riscos Cibernéticos;

- Manter atualizada a Política de Riscos Cibernéticos e instruções normativas correspondentes;

- Monitorar a exposição dos negócios da Porto a riscos e ameaças cibernéticas;

- Acompanhar a implementação de planos de ação ou medidas corretivas que visem sanar deficiências que possam expor o negócio a riscos cibernéticos;

- Orientar as unidades operacionais (1ª Linha de Defesa) e Diretoria da Companhia em relação à gestão de riscos cibernéticos;

- Realizar teste dos controles identificados, a fim de confirmar o entendimento da estrutura dos controles que mitigam os pontos de risco;

- Obter e armazenar evidência dos testes dos controles avaliados, de acordo com os critérios de amostragem e periodicidade definida;

- Reportar as alçadas competentes os riscos identificados que apresentem fragilidade ou inexistência de controle, os quais deverão apresentar planos de ação para mitigação. Acompanhar/ realizar follow-up dos planos de ação com foco na adequação dos controles internos (desenho ou efetividade dos controles), incluindo pontos de auditoria interna, auditoria externa, fiscalizações e demais demandas para adequação das estruturas;

- Elaborar os relatórios que permitam a identificação e correção tempestiva das deficiências dos controles.

9.9 Controles Internos e Compliance

- Garantir o atendimento às normas publicadas pelos órgãos reguladores.

- Auxiliar as áreas de negócios no atendimento às demandas dos reguladores externos.
- Orientar os colaboradores a efetuar os treinamentos relacionados à Governança Corporativa e Compliance.

9.10 Auditoria interna

- Avaliar a adequação da Estrutura de Gestão de Riscos, dentro de um ciclo máximo de três anos.
- Zelar pela conformidade das políticas, normas, padrões, procedimentos e regulamentações internas e externas.
- Recomendar aprimoramentos no ambiente de controles internos.

9.11 Colaboradores, terceiros e parceiros de serviço

- Seguir as diretrizes estabelecidas nesta política;
- Atuar de maneira integrada com as áreas de controle para prevenção e apoio na resposta de eventuais incidentes que causam dados as estratégias de negócio;
- Reportar incidentes e desvios de condutas (conforme código de conduta da companhia) identificados às áreas de segurança da informação, de riscos cibernéticos ou canais de denúncia;
- Identificar e tratar as informações conforme sua classificação e em linha com as políticas e normativas da Porto;
- Ser responsável sobre as informações classificadas como “confidenciais”, “privadas”, “internas” e “públicas” da Porto.

10. VIGÊNCIA

Esta Política entrará em vigor na data de sua publicação e será revisada periodicamente, sendo passível de alteração ou atualização sempre que constatada sua necessidade.

11. VIGÊNCIA

Esta Política entrará em vigor na data de sua publicação e será revisada periodicamente, sendo passível de alteração ou atualização sempre que constatada sua necessidade.

12. APROVAÇÃO

Esta Política foi revisada e aprovada pela Diretoria responsável e será arquivada na sede da Sociedade.

Setembro/2022