Política de Segurança da Informação e Cibernética para Terceiros

A Política de Segurança da Informação e Cibernética do Banrisul tem por objetivo estabelecer as diretrizes fundamentais a serem adotadas para proteger os dados e informações do Banrisul e de seus clientes, bem como os sistemas e ativos que os mantêm. Ela orienta a empresa a prevenir, identificar, avaliar, monitorar, combater e tratar ou mitigar os principais fatores geradores de risco cibernético e de segurança da informação.

Segurança da informação é a garantia de que as informações estarão sempre protegidas, mantidas íntegras e disponíveis apenas àqueles com direito de acessá-las. As disciplinas de segurança da informação abordam todos os tipos de controles para tornar isso possível, desde ferramentas lógicas, como criptografia e chaves de acesso, até controles físicos, como restrição de acesso ao Datacenter e posicionamento de equipamentos.

Segurança cibernética é a salvaguarda das pessoas, da sociedade, das organizações e das nações contra riscos cibernéticos. Trata-se de um subconjunto da segurança da informação, que aborda de forma mais enfática as ferramentas lógicas de proteção.

O conteúdo abaixo está dividido em Princípios, e contempla, de forma resumida, as principais práticas de segurança cibernética e de segurança da informação a serem seguidas por Terceiros, conforme nossa Política de Segurança da Informação e Cibernética, aprovada em reunião do Conselho de Administração em 11 de dezembro de 2024. Estes devem documentar e implementar mecanismos, processos, procedimentos e controles para atender os itens desse documento, aplicáveis exclusivamente ao seu escopo de prestação de serviços/objeto do contrato.

Para fins desse documento, Terceiro é toda e qualquer empresa fornecedora de produtos, prestadora de serviços, bem como seus respectivos prepostos e colaboradores, que possua contrato que envolva armazenamento, processamento ou tratamento de dados ou informações de propriedade das empresas controladas do Grupo Banrisul, nominadas nesse documento como ‘Banrisul’.

Este documento é atualizado pelo menos anualmente. Consequentemente, diretrizes aqui contidas podem ser modificadas. O Banrisul disponibiliza e mantém esta versão atualizada para informar os Terceiros e seus colaboradores.

Princípios Gerais para a Segurança dos Dados e Informações

CLASSIFICAÇÃO

O Terceiro deve respeitar a classificação dos dados e informação atribuída pelo Banrisul e, quando essa classificação não estiver disponível, deve tratar os dados e informações do Banrisul como confidenciais.

O uso de soluções de Inteligência Artificial, com quaisquer tipos de informações de propriedade do Banrisul, será permitido somente mediante formal e expressa autorização do Banco.

PROTEÇÃO

Os dados e informações de propriedade do Banrisul devem ser protegidos, desde o momento de sua criação, contra acesso, modificação, subtração, destruição ou divulgação não-autorizada. Para tal, orientamos a utilização de mecanismos que garantam:

- **Confidencialidade:** devem ser aplicados mecanismos de preservação da confidencialidade adequados para cada tipo de dado e informação transmitido, processado ou armazenado, evitando sua utilização indevida.
- **Integridade:** devem ser aplicados mecanismos de preservação da integridade adequados para cada tipo de dado e informação transmitido, processado ou armazenado, evitando sua adulteração.
- **Autenticidade:** devem ser aplicados mecanismos de preservação da autenticidade, adequados para cada tipo de dado e informação transmitido, processado ou armazenado, garantindo sua legitimidade e não-repúdio.
- **Disponibilidade:** devem ser mantidas cópias de segurança dos dados e informações utilizados por sistemas críticos, em ambientes protegidos e gerenciados, mantendo a disponibilidade aos seus proprietários em caso de necessidade de restauração por período razoável de tempo.
- **Rastreabilidade:** devem ser aplicados mecanismos adequados para cada tipo de dado e informação a ser protegido, e informações de rastreabilidade devem ser mantidas por tempo razoável, conforme as necessidades de auditoria e atendimento às legislações vigentes.
- **Outras proteções:** declaradas nos demais Princípios ao longo dessa Política.

Princípios para a Segurança dos Recursos Humanos

CONTRATAÇÃO SEGURA DE RECURSOS HUMANOS

O Terceiro deve possuir e apresentar Política de Segurança da Informação e Cibernética aos seus colaboradores e manter com eles acordos sobre seus papéis e responsabilidades na segurança da informação, em forma de termos, acordos ou declarações de confidencialidade e sigilo que devem ser assinados pelos mesmos.

SIGILO PROFISSIONAL

Os colaboradores do Terceiro devem manter absoluto sigilo profissional, zelando pela proteção dos dados e informações do Banrisul a que tenham acesso.

Não é permitida a gravação de reuniões de trabalho ou eventos, sejam eles nas dependências do Banco ou em sistemas de videoconferência, salvo expressa autorização para assim proceder. Por analogia, também não é permitida a gravação de reuniões envolvendo assuntos contratuais do Banrisul, nas dependências de Terceiros.

USO RESPONSÁVEL DOS RECURSOS DO BANRISUL

Os colaboradores do Terceiro são responsáveis pela utilização dos recursos, tecnológicos ou não, disponibilizados pelo Banrisul para o desempenho de suas atribuições na prestação de serviços para o Banco, em consonância com as regras estabelecidas em contrato.

As senhas utilizadas para acesso aos recursos são pessoais, intransferíveis e devem ser escolhidas e renovadas atendendo às melhores práticas orientadas pela área de Segurança da Informação do Banrisul.

Não é permitido que mecanismos de segurança instalados nos recursos tecnológicos de propriedade do Banrisul sejam desabilitados ou desinstalados sem a expressa autorização dos gestores das áreas de Tecnologia do Banco.

Não é permitido o uso de sistemas e aplicativos instalados localmente ou que funcionem de forma on-line através da Internet que não tenham sido expressamente autorizados ou disponibilizados pelos gestores das áreas de Tecnologia do Banco.

Não é permitido o envio ou armazenamento de dados e informações do Banrisul por intermédio de sistemas e aplicativos de forma on-line através da Internet ou mediante o uso de mídias de armazenamento portátil.

Não é permitido o uso dos recursos tecnológicos fornecidos pelo Banrisul para fins particulares.

CULTURA E CONSCIENTIZAÇÃO

Todos os colaboradores admitidos para atuar nos contratos firmados com o Banrisul devem estar cientes e comprometidos com o seu papel na proteção dos dados, das informações e dos recursos do Banrisul a que tiverem acesso, tecnológicos ou não. Orienta-se que os colaboradores sejam avaliados periodicamente em relação ao cumprimento de seus papéis e funções relacionados à segurança da informação.

O Banrisul pode disponibilizar, durante o período contratual, material de conscientização associado a esta ou futuras versões desta Política. A utilização deste material, pelos Terceiros, é obrigatória.

Princípios para a Segurança dos Negócios

CONCEPÇÃO DE PRODUTOS E SERVIÇOS SEGUROS

Todos os novos produtos e serviços desenvolvidos por Terceiros para uso do Banrisul devem passar por avaliação dos aspectos de segurança cibernética e da informação. A avaliação inicial deve ser realizada pelo Terceiro e posteriormente pelo gestor do contrato, à luz dos itens desta Política e, caso sejam identificadas questões de segurança da informação, a área de Segurança da Informação do Banrisul deve ser consultada.

MANUTENÇÃO DE AMBIENTES DE NEGÓCIO SEGUROS

Todos os ambientes de negócio mantidos por Terceiros em atendimento a contratos com o Banrisul, como salas de atendimento, salas de negócios, unidades ou áreas administrativas, devem proporcionar a proteção contínua dos dados e informações da empresa através da manutenção de ambientes seguros para o atendimento de nossos clientes, a realização de negócios e a realização das atividades administrativas e operacionais.

ESCOLHA SEGURA DE PARCEIROS DE NEGÓCIO

O Terceiro deve escolher e contratar parceiros de negócio capacitados a atender sua Política de Segurança da Informação e Cibernética naquilo que for aplicável. Nesse sentido, deve ser observado pelo Terceiro em quaisquer contratações que envolvam prestação de serviços para o Banrisul, no mínimo, o cumprimento dos Princípios declarados neste documento.

Princípios para a Segurança no Desenvolvimento de Software

DESENVOLVIMENTO SEGURO

Os sistemas e aplicativos desenvolvidos para uso do Banrisul e de seus clientes devem ser feitos à luz dos padrões internos de desenvolvimento de sistemas, infraestrutura de TI e segurança da informação vigentes, buscando que sejam protegidos da melhor forma possível de exploração maliciosa por ameaças de quaisquer origens. Devem ser também

consideradas as melhores práticas de desenvolvimento de software existentes no mercado. Os detalhes sobre esse processo podem ser consultados junto à área de Segurança da Informação do Banrisul.

ANÁLISE DE VULNERABILIDADE EM CÓDIGOS-FONTE

Os sistemas e aplicativos para uso do Banrisul e de seus clientes devem ter seu código avaliado quanto à existência de vulnerabilidades de segurança. Os detalhes sobre esse processo podem ser consultados junto à área de Segurança da Informação do Banrisul.

TESTES E HOMOLOGAÇÕES SEGUROS

Os sistemas e aplicativos para uso do Banrisul e de seus clientes devem ser desenvolvidos e testados em ambientes logicamente segregados e passar por testes padronizados que assegurem a funcionalidade e a segurança dos mesmos. Os testes devem ser realizados não somente pelos desenvolvedores e testadores, mas também pelos gestores dos sistemas ou aplicativos que estão sendo desenvolvidos. Os detalhes sobre esse processo podem ser consultados junto à área de Segurança da Informação do Banrisul.

IMPLANTAÇÃO SEGURA

Devem ser aplicados métodos de ofuscação de código e assinatura de código antes que o sistema ou aplicativo esteja pronto para implantação. A implantação de um sistema ou aplicativo deve sempre aplicar o Princípio de Gestão de Mudanças, com a aprovação de todas as áreas eventualmente afetadas por essa implantação, salvo situações excepcionais em que a continuidade do negócio esteja em risco.

Na primeira implantação de um sistema ou aplicativo que envolva dados ou informações do Banrisul, deve haver garantia de que a segurança desse sistema ou aplicativo tenha sido avaliada à luz desta política. Essa avaliação se aplica também à implantação de melhorias que alterem significativamente a segurança de um sistema ou aplicativo já em produção.

Princípios para a Segurança do Ambiente Tecnológico

PROTEÇÃO FÍSICA DO AMBIENTE TECNOLÓGICO

Os datacenters do Terceiro devem estar fisicamente segregados do restante de suas instalações e devem ser utilizados mecanismos de controle de acesso físico, para assegurar a proteção dos ativos de infraestrutura que suportam os sistemas e aplicativos do Banrisul contra acessos físicos não-autorizados.

Outros ambientes tecnológicos que existam fora dos datacenters e que necessitem de proteção física, como salas-cofre, devem receber o nível de proteção física adequada à sensibilidade dos dados e informações que estão protegendo.

PROTEÇÃO LÓGICA DO AMBIENTE TECNOLÓGICO

As redes lógicas internas (acessíveis apenas internamente) e externas (acessíveis através da Internet) devem ser logicamente segregadas no menor nível de granularidade que for tecnicamente possível, utilizando mecanismos de proteção de perímetro que garantam a proteção do ambiente tecnológico de acessos lógicos não-autorizados.

AUTENTICAÇÃO E GESTÃO DE ACESSOS

A gestão de acessos deve basear-se no princípio do menor privilégio, isto é, todo acesso aos equipamentos de tecnologia, áreas de armazenamento lógico, sistemas e aplicativos que compõem o ambiente computacional deve ser concedido sob necessidade justificada e

apenas durante o tempo necessário, de acordo com o papel do indivíduo dentro do processo e respeitando a apropriada segregação de funções. Os acessos devem ser revisados periodicamente pelos gestores responsáveis por sua concessão.

Todos os acessos a ativos de tecnologia e sistemas internos e externos devem ser autenticados, e o uso de senhas e métodos de autenticação deve seguir os padrões definidos pela área de Segurança da Informação do Banrisul.

Sempre que a tecnologia (hardware) ou o método de programação utilizado (software) oferecer suporte para tal, os acessos aos sistemas e aplicativos devem ser efetuados utilizando métodos de autenticação de múltiplos fatores, bem como, quando for o caso, mecanismos de single sign-on ligados ao sistema de gestão de acessos do Banrisul. Os detalhes sobre esse processo podem ser consultados junto à área de Segurança da Informação do Banrisul.

USO DE CRIPTOGRAFIA E CERTIFICAÇÃO DIGITAL

A proteção dos dados e informações baseia-se, em grande medida, no uso de criptografia e certificação digital. Devem ser aplicadas, pelo Terceiro, as técnicas de criptografia forte e certificação digital definidas pela área de Segurança da Informação do Banrisul, tanto no desenvolvimento de sistemas e aplicativos quanto na configuração dos bancos de dados e equipamentos que realizem a transmissão ou armazenamento desses dados e informações.

ADOÇÃO SEGURA DE TECNOLOGIAS

Recomenda-se que todo projeto para adoção de tecnologia pelo Terceiro para atender ao Banrisul passe por avaliação dos aspectos de segurança cibernética e da informação. A avaliação inicial deve ser realizada pelo Terceiro junto ao gestor do contrato à luz dos itens desta Política e, caso sejam identificadas questões de segurança da informação, a área de Segurança da Informação do Banrisul deve ser envolvida.

PROTEÇÃO CONTRA SOFTWARES MALICIOSOS

O Terceiro deve adotar mecanismos de detecção e remoção de softwares maliciosos em todos os ativos de tecnologia nos quais esta medida seja aplicável para prevenir e dar visibilidade a eventuais tentativas de instalação de softwares maliciosos por agentes de ameaça.

GESTÃO DE VULNERABILIDADES

O Terceiro deve manter estratégias e executar ações preventivas que permitam a gestão de vulnerabilidades em seu ambiente tecnológico. Os detalhes sobre esse processo podem ser consultados junto à área de Segurança da Informação do Banrisul.

PREVENÇÃO, DETECÇÃO E CONTENÇÃO DE INTRUSÕES

O Terceiro deve implementar mecanismos de prevenção e detecção de intrusão nos perímetros de seu ambiente lógico, bem como em pontos estratégicos das redes interna e externa, com a finalidade de prevenir e dar visibilidade a eventuais tentativas de exploração maliciosa por agentes de intrusão. Os detalhes sobre esse processo podem ser consultados junto à área de Segurança da Informação do Banrisul.

MONITORAMENTO DO AMBIENTE TECNOLÓGICO

O Terceiro deve monitorar seu ambiente constantemente, visando a identificação de possíveis incidentes de segurança cibernética e da informação que possam estar ocorrendo ou em vias de ocorrer. Esse monitoramento deve indicar, em alguma medida, a eficácia dos mecanismos de segurança implementados pelo Terceiro. Os detalhes sobre esse processo podem ser consultados junto à área de Segurança da Informação do Banrisul.

TRATAMENTO DE INCIDENTES

O registro e tratamento de incidentes de segurança cibernética e da informação deve ocorrer de acordo com a sua relevância. O Terceiro deve compartilhar com o Banrisul informações a respeito dos incidentes de segurança cibernética e da informação que envolverem a prestação de serviço objeto do contrato entre as duas empresas. Os detalhes sobre esse processo podem ser consultados junto à área de Segurança da Informação do Banrisul.

GESTÃO DE MUDANÇAS

Deve existir no Terceiro um processo de gestão de mudanças alinhado às melhores práticas de mercado, a fim de garantir que as implantações de mudanças nos sistemas, aplicativos e ativos de infraestrutura não afetem a disponibilidade dos mesmos ou a confidencialidade e integridade dos dados e informações do Banrisul.

RECUPERAÇÃO DE DESASTRES

Os ambientes computacionais do Terceiro devem ser mantidos em configurações físicas e lógicas que busquem minimizar interrupções de produtos ou serviços que sejam causadas por indisponibilidades de ativos, sistemas ou aplicativos.

O Terceiro deve garantir que o tempo de retorno do ativo ou sistema esteja sempre dentro do limite aceitável, utilizando-se mecanismos de recuperação de desastres para não prejudicar a continuidade da prestação do serviço para o Banrisul.

Os testes dos Planos de Recuperação de Desastres devem prever cenários de incidentes cibernéticos quando aplicáveis. Os detalhes sobre esse processo podem ser consultados junto à área de Segurança da Informação do Banrisul.

Detalhes adicionais ou esclarecimentos sobre esse documento podem ser consultados junto ao gestor do contrato.