

Política de Segurança da Informação para Fornecedores

Versão: 02

Data da última revisão: 03/05/2023
Código: RGS-DTI-043-00

Esta política estabelece as diretrizes a serem seguidas pelos fornecedores da Icatu, para o correto acesso e manuseio de informações. De forma a assegurar a confidencialidade, integridade e disponibilidade destas em seu ambiente físico e lógico.

Esta política é aplicável aos Prestadores de serviço que geram ou manipulam informações de propriedade e/ou sob guarda das empresas: Icatu Seguros S.A.; Icatu Capitalização S.A.; Vanguarda Companhia de Seguros Gerais; Vanguarda Capitalização S.A.; Rio Grande Seguros e Previdência S.A. e Rio Grande Capitalização S.A.; Icatu Consultoria de Investimentos Ltda.; Icatu Assessoria Ltda. (“Grupo Icatu Seguros”), Icatu Vanguarda Gestão de Recursos Ltda; e Icatu Fundo Multipatrocinado, denominadas em conjunto "Icatu".

ACEITAÇÃO DA POLÍTICA DE SI PARA FORNECEDORES



Ao iniciar as atividades de prestação de serviço que envolvam informações da Icatu, os Fornecedores devem ter acesso a “Política de Segurança da Informação para Fornecedores” e fornecer de acordo via plataforma, visando documentar o seu comprometimento em manter a segurança e atender aos requisitos definidos, conforme aplicável, realizando a divulgação a todos os envolvidos nas atividades relacionadas a prestação de serviços a Icatu.

DESCUMPRIMENTO DA POLÍTICA DE FORNECEDORES



Caso seja identificado o descumprimento referente a esta Política, a Icatu poderá revogar os acessos e avaliar as violações para definir as ações necessárias conforme estabelecido no contrato de prestação de serviço firmado entre a Icatu e o Fornecedor.

Esta política não anula e não substitui o contrato estabelecido entre as partes



As seguintes diretrizes devem ser seguidas e consideradas em todas as atividades realizadas dentro ou fora das dependências da Icatu, sempre que exista a necessidade de manipulação de suas informações:

- ✓ Todas as atividades inerentes à Segurança da Informação devem estar em conformidade com esta Política de Segurança da Informação para Fornecedor da Icatu;
- ✓ Todos os recursos e informações devem ser protegidos de forma a resguardar a confidencialidade, integridade e disponibilidade;
- ✓ Todo o acesso deve ser único e manter trilhas de auditoria contendo, no mínimo, endereço IP de origem da chamada, porta de comunicação origem da chamada (porta TCP do cliente), data, hora, sistema, usuário (quando aplicável), objeto, falha ou sucesso da ação das configurações realizadas nos sistemas e meios relacionados a prestação de serviço, observadas a legislação e regulamentações vigentes.
- ✓ Todos os Fornecedores envolvidos nas atividades da Icatu devem estar cientes da presente Política de Segurança da Informação para Fornecedores, assim como possuir suas próprias políticas de segurança da informação, controle de acesso lógico, dispositivos móveis, mídias removíveis, continuidade da segurança da informação, gestão de mudanças, gestão de incidentes, mesa e tela limpas e outras;
- ✓ Todos os contratos com fornecedores ou prestadores de serviço que envolvam: Serviços de tecnologia, Manipulação de dados ou Tecnologia, devem conter o Anexo Requisitos de Segurança da Informação para Fornecedores e Prestadores de Serviços, podendo haver alteração dos requisitos presentes no anexo conforme o escopo contratado;
- ✓ Todos os equipamentos que processam informações pertencentes a Icatu devem possuir solução antivírus atualizada, controles de acesso remoto, incluindo, mas não se limitando a, autenticação de dois fatores, acesso ao dispositivo por VPN (Virtual Private Networking), e portas de protocolos restritos;
- ✓ Não é permitida a realização de testes de invasão, *brute force* ou qualquer ação que esteja caracterizada como acesso indevido.

PRINCÍPIOS GERAIS



- ✓ Qualquer equipamento que necessite de acesso contínuo as informações e ambientes da Icatu devem possuir o nosso software de *Endpoint Detection and response* (EDR) instalado;
- ✓ Para acesso ao ambiente da Icatu, o equipamento do Fornecedor deverá possuir um Sistema Operacional licenciado e atualizado com todas as correções de segurança e um software de Antivírus com atualização das vacinas recorrentes.

RESPONSABILIDADE DOS FORNECEDORES



Os fornecedores se obrigam à:

- ✓ Manter-se atualizado sobre a Política de Segurança da Informação da Icatu disponibilizada no Portal do Fornecedor;
- ✓ Responder a *due dilligence* de segurança sempre que solicitado;
- ✓ Cumprir o Plano de Ação para os Fornecedores, sendo o caso;
- ✓ Sendo o caso, permitir a realização de Teste de Penetração nas Aplicações que farão o armazenamento, coleta ou transmissão das informações da Icatu;
- ✓ Comprometer-se em manter a segurança e atender aos requisitos definidos nesta Política;
- ✓ Possuir os requisitos de controles administrativos, físicos e técnicos aptos a garantir a Segurança das Informações da Icatu.
- ✓ Realizar a divulgação da Política de Segurança da Informação para Fornecedores aos profissionais que realizarão atividades na Icatu.
- ✓ Celebrar junto a seus colaboradores, terceiros e outras pessoas que possam vir a ter contato com as Informações da Icatu, os instrumentos pertinentes de acordo de sigilo e confidencialidade, bem como, em caso de solicitação apresentar a documentação comprobatória de que seus Prepostos têm ciência das regras de confidencialidade e Segurança da Informação da Icatu.
- ✓ Assegurar que possuem salvaguardas para o gerenciamento, aquisição e suporte à segurança da informação em serviços de nuvem;



RESPONSABILIDADE DOS FORNECEDORES

- ✓ Manter seus colaboradores conscientizados periodicamente de acordo com os procedimentos de segurança da informação, bem como orientados devidamente de seus papéis e responsabilidades;
- ✓ Manter um inventário atualizado dos ativos de Hardware e Softwares;
- ✓ Não permitir a utilização de equipamentos não monitorados para a prestação de serviços;
- ✓ Não causar qualquer tipo de embaraço à atuação da SUSEP, permitindo a consulta aos dados objeto do contrato, às informações referentes aos serviços prestados e aos contratos e acordos firmados para a sua execução incluindo o possível acesso às suas dependências quando solicitado pela SUSEP, sendo o caso.
- ✓ Todos os Fornecedores se comprometem a notificar e informar a Icatu sobre a subcontratação de serviços relevantes no prazo máximo de 5 (cinco) dias úteis;
- ✓ Responder no prazo máximo de 15 (quinze) dias úteis a avaliação de segurança da informação, quando solicitado;
- ✓ Criptografar as comunicações de acesso remoto para sistemas ou aplicações que contenham dados da Icatu e deve possuir controles, incluindo, mas não se limitando a, autenticação de dois fatores, acesso ao dispositivo por Virtual Private Networking (VPN) e portas de protocolos restritos;
- ✓ Garantir que dos dispositivos que terão acesso as informações da Icatu possuem um Sistema Operacional licenciado e atualizado com todas as correções de segurança e um Software de Antivírus com atualização das vacinas recorrentes.



PROPRIEDADE DA INFORMAÇÃO

Toda informação produzida dentro ou fora da Icatu a respeito de seus dados, clientes, fornecedores e negócio é considerada de sua propriedade, não importando a data de criação ou forma de representação e transporte. A confidencialidade das informações criadas ou acessadas deve ser mantida mesmo após encerramento das relações comerciais.

O cumprimento desta Política de Segurança da Informação e a preservação da confidencialidade das informações, dados, dados pessoais e dados pessoais sensíveis da Icatu é um dever de todos. É vedada a reprodução de quaisquer documentos, dados ou informações da Icatu sem o expresse consentimento desta por meio de autorização de representante com poderes para tanto.



CLASSIFICAÇÃO DA INFORMAÇÃO

As informações de propriedade da Icatu devem ser utilizadas exclusivamente para os propósitos estabelecidos no instrumento contratual. Todas as informações enviadas ao Fornecedor devem ser tratadas como confidenciais.

O Fornecedor deve possuir e implementar critérios de classificação e rotulagem das Informações, sempre tratando as informações recebidas da Icatu como “Confidenciais”. O manuseio de qualquer informação independente de sua classificação deve ocorrer com o mínimo de exposição, no que se refere ao armazenamento/transmissão e descarte.

DESCARTE DA INFORMAÇÃO



Os Fornecedores devem se comprometer a implementar Políticas e Procedimentos para garantir que a informação da Icatu seja destruída de forma segura, quando não for mais necessária para os fins autorizados. Sendo necessário, confirmar antes do descarte dos ativos que a informação da Icatu foi apagada de forma adequada, mantendo o registro da destruição.

Assim que as informações não forem mais necessárias para os fins autorizados pela Icatu, em contrato e/ou fins regulatórios, elas devem ser destruídas de forma segura, mantendo um registro para garantir que foi apagada de forma adequada.

Havendo terceiro contratado envolvido para o processamento da informação da Icatu, o Fornecedor deve garantir que este realizará o descarte de forma segura das informações, quando estas não forem mais necessárias.

SEGURANÇA NAS COMUNICAÇÕES



Os Fornecedores devem se comprometer a segregar logicamente e/ou fisicamente os dados da Icatu dos demais clientes.

Também devem assegurar a implementação de procedimentos de filtragem dos acessos à Internet para proteger as estações de trabalho do usuário final de sites mal-intencionados e transferências de arquivos não autorizados. As informações da Icatu devem ser criptografadas quando em repouso e trânsito.

As atividades de compartilhamento e transmissão da informação devem ser realizadas através dos meios seguros homologados por Segurança da Informação da Icatu, como por exemplo SFTP, Connect Direct e My File Gateway.



USO DA INTERNET

Para casos em que a atuação *in loco* seja necessária, o uso de conexões aos sistemas de internet é permitido para atender apenas aos propósitos de negócios da Icatu, que se reversa ao direito, a qualquer momento, de:

- ✓ Suspender o acesso do fornecedor;
- ✓ Restringir o download e upload de arquivos ou acesso a conteúdo que não sejam de interesse da empresa;
- ✓ Monitorar e auditar os acessos;
- ✓ Solicitar aos Fornecedores justificativas pelos acessos efetuados.

É expressamente vetado o uso dos recursos da Icatu para:

- ✓ Acesso ou veiculação de conteúdo relacionado à pedofilia, conteúdos de cunho: político, religioso, discriminatório, pornográfico e ilegal (pirataria de Software, comércio de ilícitos etc.);
- ✓ Quaisquer outras atividades consideradas inapropriadas, indevidas ou desvinculadas às atividades desempenhadas na empresa;
- ✓ Publicar, postar, carregar, distribuir ou divulgar quaisquer tópicos, nomes, materiais ou informações que incentivem a discriminação, ódio ou violência com relação a uma pessoa ou a um grupo;
- ✓ Publicar, postar, carregar, distribuir ou divulgar informações falsas;
- ✓ Utilizar-se da internet e outros serviços disponibilizados com o intuito de cometer fraude;
- ✓ Utilizar os serviços para, de qualquer modo reproduzir ou infringir direitos de terceiros, sejam imagens, áudio, fotografias, vídeos, softwares ou qualquer material protegido por lei de propriedade intelectual, incluindo, lei de direitos autorais, marcas ou patentes;
- ✓ Fins ilícitos, tais como: atividades hackers, crackers, bombas, falsidade ideológica, entre outros;
- ✓ A utilização da rede Wireless Corporativa por dispositivos não homologadas pela Icatu.

Em caso de exceção para prestadores de serviço e terceiros que desenvolverão projetos de longo prazo, é necessário abrir uma solicitação ao Service Desk, que passará pela aprovação do gestor imediato

BACKUP



Os Fornecedores devem realizar periodicamente o procedimento de execução de backups e testes de *restore* nos ativos que armazenam informações da Icatu de forma a evitar ou minimizar a perda de dados diante da ocorrência de incidentes, quando aplicável.

A Icatu exige que toda mídia armazenada fora de sua infraestrutura seja criptografada e as chaves de segurança armazenadas em um cofre corporativo.

TECNOLOGIA EM NUVEM



Aos Fornecedores que utilizam o ambiente de nuvem para a prestação do serviço, é recomendado salvaguardar o gerenciamento, a aquisição e o suporte à Segurança da Informação nesses serviços, de modo a garantir a confidencialidade, integridade e disponibilidade das informações presentes no sistema operacional.

A Icatu também orienta assegurar a criptografia dos dados em trânsito e repouso nas camadas de aplicação e de interfaces.

É indicado definir e documentar uma Política de Utilização de Serviços em Nuvem que contemple as estratégias de adesão desses serviços, visando o cumprimento da legislação e regulamentação em vigor, descrevendo como se realizará a substituição de prestadores de serviços em nuvem em caso de descontinuidade ou necessidade.

Sempre informar aos representantes da Icatu o mais rápido possível sobre a contratação de fornecedores de armazenamento e processamento de dados em nuvem, indicando qual empresa selecionada, os serviços a serem prestados e, se possível, quais os países e regiões onde os dados serão armazenados, processados e gerenciados.

CONTROLE DE ACESSO



Os Fornecedores devem possuir controles de acessos à informação a fim de protegê-la contra possíveis danos, acessos não autorizados ou perdas. Sendo assim, os Fornecedores devem possuir uma Política de Controle de Acesso que descreva as diretrizes para a criação, alteração, revisão e exclusão de contas de usuários para sistemas ou aplicativos.

Os privilégios da conta do usuário devem ser realizados com base no princípio do privilégio mínimo necessário e devem ser formalmente autorizados e registrados. Quando aplicável para a prestação do serviço, o fornecedor deve credenciar nos domínios da Icatu seus profissionais autorizados a operar presencialmente e remotamente.

O fornecedor se responsabiliza por comunicar a Icatu com antecedência de, no mínimo, 01 (um) dia útil, qualquer término ou mudança de responsabilidades de emprego de funcionários envolvidos diretamente na execução dos serviços prestados.

GESTÃO DE VULNERABILIDADE



O fornecedor deve possuir um programa corporativo de gestão de patches e vulnerabilidades para verificar se ativos de hardware e software possuem vulnerabilidades conhecidas.

Os Fornecedores devem realizar testes de segurança anuais (*Pentest*) com empresa independente, se possível, a fim de assegurar que os controles de segurança estão devidamente implementados.

Os relatórios deverão ser compartilhados com a Icatu, sempre que esta entender necessário, ficando o fornecedor responsável por solucionar todas as vulnerabilidades.

GESTÃO DE VULNERABILIDADE



O Fornecedor terá os seguintes prazos, a contar da data de comunicação da vulnerabilidade a Icatu para providenciar o plano de correção que deverá ser validado pela Icatu:

- Alta vulnerabilidade: até 07 (sete) dias;
- Média vulnerabilidade: até 14 (catorze) dias;
- Baixa vulnerabilidade: até 21 (vinte e um) dias.

A Icatu poderá solicitar a execução dos testes de Segurança da Informação (Pentest) na infraestrutura que suporta a operação, desde que comunicado previamente com 10 (dez) dias úteis de antecedência.

DESENVOLVIMENTO E MAUTENÇÃO DE SISTEMAS



Os Fornecedores devem manter controles de alteração projetados para atender aos requisitos de segurança dos sistemas de informação desenvolvidos internamente e relacionados a prestação de serviços, bem como realizar a revisão e testes de código periodicamente.

Também devem separar logicamente ambientes para desenvolvimento, teste e produção. O acesso dos usuários aos ambientes que contenham informações da Icatu deve ser restrito e segregado, com base nas responsabilidades do trabalho atribuído.

As alterações dos softwares e infraestrutura devem ser autorizadas e formalmente documentadas, testadas, revisadas e aprovadas, antes da migração do ambiente não produtivo para o ambiente de produção.

Os dados de produção da Icatu não devem ser usados para realização de testes em qualquer ambiente produtivo e/ou não produtivo.

GESTÃO DE MUDANÇA



Os Fornecedores devem possuir um processo de gestão de mudanças com o intuito de controlar as alterações nos sistemas de produção, rede de produção, aplicativos, arquivos de dados estruturais, outros componentes do sistema e mudanças físicas/ambientais, através de um registro formal de controle de mudança, minimizando os impactos e riscos associados à manutenção do serviço.

RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO



Os Fornecedores devem possuir um plano de resposta a incidentes de segurança da informação que inclua qualquer evento de Segurança da Informação que perturbe ou que possa interromper um serviço.

O plano deve detalhar os processos de tratamento de incidentes para detectar, triar, responder e gerir o pós-incidente que afete as redes e/ou sistemas.

Além disto, o fornecedor deverá informar a Icatu em, no máximo 24 horas, após o conhecimento do incidente de segurança de qualquer natureza envolvendo informações da Icatu através do endereço de e-mail **csirt@icatusseguros.com.br**, contendo as seguintes informações:

- ✓ Data e hora do incidente;
- ✓ Data e hora da ciência do incidente;
- ✓ Qual o tipo de incidente de segurança;
- ✓ Descrição do incidente;
- ✓ No caso de incidente envolvendo dados pessoais, a descrição da natureza dos dados pessoais afetados e as informações sobre os titulares envolvidos;
- ✓ Indicação das medidas técnicas e de segurança tomadas para resposta ao incidente e ações para evitar novos incidentes;
- ✓ Riscos relacionados ao incidente;
- ✓ As medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do incidente.

RESPOSTA A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO



Na ocorrência de mais de um Incidente de Segurança no período de 90 (noventa) dias corridos, a Icatu poderá exigir que o fornecedor, às suas expensas, contrate uma empresa de segurança aprovada pela Icatu para avaliar as suas medidas protetivas. O fornecedor deverá compartilhar o relatório de avaliação a Icatu e se comprometer a corrigir todas as vulnerabilidades identificadas durante a avaliação.

Se o fornecedor, seus colaboradores ou terceiros forem responsáveis por um incidente de segurança, independentemente de este ocorrer por descumprimento do Contrato ou falha em notificar a Icatu, este se compromete a reembolsar a Icatu por todos os danos e custos devidos em razão dos atos e/ou omissões e pagará pelas despesas incorridas na investigação e remediação do incidente de segurança.

CONTINUIDADE DA SEGURANÇA DA INFORMAÇÃO



O fornecedor deve manter a continuidade das operações de Segurança da Informação a fim de minimizar as perdas e manter a operacionalidade dos sistemas em situações adversas como por exemplo, situações de crise ou desastre.



DILIGÊNCIA E ANÁLISE DE RISCOS

Os Fornecedores devem permitir que a Icatu avalie os serviços contratados por meio de diligências, desde que avisada previamente com mínimo de 10 (dez) dias úteis, a aderência aos requisitos contratuais, incluindo os controles de Segurança da Informação, comprometendo-se a disponibilizar sua documentação, relatórios e/ou informação comprobatória durante a diligência.

Os Fornecedores que possuem o escopo do serviço a ser contratado devidamente certificado pela ISO 27001 não precisarão realizar o processo completo de diligência e análise de riscos, desde que apresentem a comprovação da vigência da certificação para o escopo contratado e a mesma seja validada pela área de Segurança da Informação da Icatu.

SEGURANÇA NO RELACIONAMENTO COM O FORNECEDOR



Os fornecedores devem assegurar que seus subcontratados e prestadores de serviços, com acesso à informação da Icatu, possuam minimamente os mesmos controles e procedimentos de Segurança da Informação descritos nesta Política.

Os acordos com essas partes devem ser revisados periodicamente para assegurar que a segurança da informação e os requisitos de proteção de dados permanecem apropriados.

DISPOSIÇÕES FINAIS



Violações a presente Política devem ser reportadas através do e-mail: csirt@icatusseguros.com.br.

* * *