ICATU

Política de Segurança da Informação para Fornecedores

PL-DTI-003-04

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.

PRINCÍPIOS GERAIS

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;
- ✓ 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.
- ✓ 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;
- ✓ Os contratos com fornecedores ou prestadores de serviço que envolvam: Serviços de tecnologia, Manipulação de dados ou Tecnologia, devem conter cláusula contratual de ciência desta Política de Segurança para Fornecedores.
- ✓ 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.
- ✓ 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.

PRINCÍPIOS GERAIS

- ✓ 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.
- ✓ Fica vetado a qualquer fornecedor a realização de testes em sistemas e aplicações, bem como a realização de quaisquer atividades de mitigação ou contenção de suspeitas ou ameaça confirmada, desde que autorizada pela área de Segurança da Informação da Icatu.

INTRODUÇÃO AO SGSI

- ✓ O Sistema de Gestão de Segurança da Informação (SGSI) tem por objetivo garantir a adoção de medidas alinhadas com as estratégias de negócio, realizando o monitoramento dos processos e ações buscando a melhoria contínua e proteção do ambiente.

- ✓ A Icatu estabeleceu seu sistema de gestão baseado na norma ISO/IEC 27001, definida como um padrão internacional, voltada para Segurança da Informação (SI), que define diretrizes para estabelecer, implementar, manter, monitorar e gerenciar um Sistema de Gestão Segurança da Informação (SGSI).

RESPONSABILIDADE DOS FORNECEDORES

- ✓ Comprometer-se a manter o nível de segurança estabelecido nos requisitos definidos na Política de Segurança da Informação para Fornecedores da Icatu, disponível no Portal do Fornecedor, e manter-se atualizado sobre esta política;
- ✓ Responder a *due diligence* de segurança sempre que solicitado;
- ✓ Possuir os requisitos de controles administrativos, físicos e técnicos aptos a garantir a Segurança das Informações da Icatu;

RESPONSABILIDADE DOS FORNECEDORES

- ✓ Manter os colaboradores conscientizados sobre os procedimentos de segurança da informação e orientados sobre seus papéis e responsabilidades. Divulgar a Política de Segurança da Informação para Fornecedores aos profissionais que atuarão na Icatu. Celebrar acordos de sigilo e confidencialidade com todos que possam ter contato com as informações da Icatu. Apresentar, quando solicitado, a documentação que comprove que os prepostos conhecem as 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;
- ✓ Manter um inventário atualizado dos ativos de *Hardware* e *Softwares*;
- ✓ Não permitir a utilização de equipamentos não monitorados para a prestação de serviços;
- ✓ Responder no prazo máximo de 15 (quinze) dias úteis à avaliação de segurança da informação e, quando solicitado, responder a questões relacionadas a incidentes de segurança da informação em até 24 horas;
- ✓ 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.

ASPECTOS GERAIS

Para que os objetivos de Segurança da Informação sejam alcançados, 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;

ASPECTOS GERAIS

- ✓ 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.
- ✓ 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;
- ✓ Os contratos com fornecedores ou prestadores de serviço que envolvam: Serviços de tecnologia, Manipulação de dados ou Tecnologia, devem conter cláusula contratual de ciência desta Política de Segurança para Fornecedores.
- ✓ 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.
- ✓ 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.
- ✓ Fica vetado a qualquer fornecedor a realização de testes em sistemas e aplicações, bem como a realização de quaisquer atividades de mitigação ou contenção de suspeitas ou ameaça confirmada, desde que autorizada pela área de Segurança da Informação da Icatu.

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 para Fornecedores e a preservação da confidencialidade das informações da Icatu é um dever de todos. É vetada a reprodução de quaisquer documentos, dados ou informações da Icatu sem o expresso 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 deverá 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 reserva 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 prover a confidencialidade, integridade e disponibilidade das informações presentes em todos os recursos de nuvem.

Em casos de substituição de prestadores de serviços em nuvem — seja por descontinuidade, encerramento contratual ou necessidade estratégica — deve ser acordado com o fornecedor o procedimento aplicável aos dados, que pode incluir devolução, portabilidade ou exclusão, conforme viabilidade legal.

A Icatu reconhece três modelos principais de serviços em nuvem:

- ✓ Infraestrutura como Serviço (IaaS) e Plataforma como Serviço (PaaS): A Icatu priorizará fornecedores classificados como estratégicos e líderes de mercado para prestação de serviços em nuvem. Durante o ciclo de gestão do fornecedor, este deve possuir certificação ISO/IEC 27001 ou SOC 2 válida, e políticas de segurança como evidência de conformidade com boas práticas de segurança da informação.

- ✓ Software como Serviço (SaaS): Conforme o escopo de análise de segurança da informação, os fornecedores devem demonstrar a adoção de controles de segurança adequados, preferencialmente com certificações reconhecidas ou evidências de conformidade com padrões de mercado. A Icatu também orienta assegurar a criptografia dos dados em trânsito e repouso nas camadas de aplicação e de interfaces.

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 de forma imediata, qualquer término ou mudança de responsabilidades de emprego de funcionários envolvidos diretamente na execução dos serviços prestados.

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 produtivo e não produtivo. 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 produtivo.

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

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.

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 15 (quinze) dias;
- ✓ Média vulnerabilidade: até 30 (trinta) dias;
- ✓ Baixa vulnerabilidade: até 60 (sessenta) dias.

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

GESTÃO DE MUDANÇAS

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 (vinde e quatro) horas, após o conhecimento do incidente de segurança de qualquer natureza envolvendo informações da Icatu através do endereço de e-mail csirt@icatuseguros.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 SEGURANÇA DA INFORMAÇÃO

Os Fornecedores devem responder a avaliação de maturidade em Segurança da Informação dos serviços contratados através do questionário enviado pela Icatu, comprometendo-se a disponibilizar documentação, relatórios e/ ou informação comprobatória que for necessária, incluindo a aderência aos requisitos contratuais.

Os Fornecedores que possuírem 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 DA INFORMAÇÃO PARA FORNECEDORES DE INTELIGÊNCIA ARTIFICIAL

Os fornecedores que desenvolvem ou utilizam inteligência artificial (IA) para a Icatu devem seguir os requisitos abaixo, para ofertar proteção das informações, conformidade com regulamentações e a integridade dos sistemas/ aplicações.

- ✓ Proteção de Dados: Deve possuir mecanismo para proteger as informações e estar em conformidade com legislações e direcionadores de órgãos reguladores.
- ✓ Desenvolvimento de Código: Realizar revisões de código regulares para identificar e corrigir vulnerabilidades de segurança.
- ✓ Controles de Acesso: Restringir o acesso apenas para usuários autorizados, com autenticação e monitoramento constante para prevenir acessos não autorizados.
- ✓ Transparência: Ações de tomada de decisão da IA devem ser transparentes e auditáveis, permitindo a rastreabilidade das decisões tomadas pela IA.
- ✓ Risco: Quando aplicável realizar avaliações de risco para identificar e mitigar potenciais vulnerabilidades nos sistemas de IA, incluindo a possibilidade de viés e erros de decisão.
- ✓ Documentação: Manter documentação sobre o desenvolvimento e uso de IA, incluindo decisões de design e justificativas.

PRESTAÇÃO DE SERVIÇOS RELEVANTES DE PROCESSAMENTO OU ARMAZENAMENTO DE DADOS

Conforme a Circular SUSEP nº 638/2021, em caso de terceirização de serviços de processamento e armazenamento de dados, os Fornecedores contratados pela Icatu que armazenam e processam dados relevantes são avaliados sob o ponto de vista de segurança da informação e segurança cibernética e devem atender e cumprir as disposições desta Política de Segurança da Informação para Fornecedores.

PRESTAÇÃO DE SERVIÇOS RELEVANTES DE PROCESSAMENTO OU ARMAZENAMENTO DE DADOS

Para estes casos o Fornecedor se compromete em não causar qualquer tipo de embaraço à atuação da Superintendência de Seguros Privados - 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.

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.

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.

DISPOSIÇÕES FINAIS

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

* * *