1 OBJETIVO

Estabelecer disposições adicionais sobre os controles mínimos de segurança e tecnologia da informação, visando a proteção das informações, ativos de informação e sistemas da Raízen.

2 ESCOPO E APLICAÇÃO

O fornecedor deve assegurar a implantação de controles de segurança da informação que atendam aos requisitos delineados abaixo e dar prova objetiva da sua existência para a Raízen, sempre que solicitado.

Controles adicionais poderão ser exigidos e/ou recomendados dependendo da natureza do contrato, relevância dos serviços ou classificação das informações a que o fornecedor tem acesso.

Esses requisitos aplicam-se a todo ambiente computacional, infraestrutura, colaboradores, terceiros e outros recursos que suportem, direta ou indiretamente, o fornecedor na prestação do serviço.

Os controles listados abaixo nos subitens 2.1 a 2.12 são requisitos mínimos necessários, alinhados e aderentes aos principais normativos, resoluções de mercado, a serem aplicados nos ambientes dos fornecedores para proteção das informações, não estando limitados a:

2.1 POLÍTICA E ORGANIZAÇÃO DE SEGURANÇA DA INFORMAÇÃO

O fornecedor deve possuir políticas de segurança da informação aprovadas e disseminadas para todos os colaboradores, expressando suas orientações e apoio, inclusive da alta direção, quanto à segurança da informação e a relação com os requisitos do negócio, leis e regulamentações relevantes.

O fornecedor deve nomear um representante com qualificação técnica apropriada e disponibilidade para coordenar as atividades e demandas relacionadas com segurança da informação na prestação dos serviços e atuar como ponto focal para os temas relacionados junto a Raízen.

2.2 GESTÃO DE ATIVOS DE INFORMAÇÃO

O fornecedor deve realizar a gestão dos ativos de informação, no que tange à sua identificação, e definição de papéis e responsabilidades de seus colaboradores para assegurar que as informações recebam um nível adequado de proteção (divulgação não autorizada, modificação, remoção ou destruição), alinhado à classificação das informações atribuída pela Raízen.

No caso dos ativos de informação do fornecedor, o fornecedor concorda em conceder acessos privilegiados, como administradores de domínios, recursos de rede e telecomunicações, aplicações, banco de dados e outros recursos de infraestrutura crítica do fornecedor mediante necessidade, solicitação e aprovação formal, de que estejam de acordo com os papéis e responsabilidades de cada colaborador e que o uso seja revisado periodicamente.

No caso dos ativos de informação da Raízen, o fornecedor entende e concorda que acessos privilegiados, como administradores de domínios, recursos de rede e telecomunicações, aplicações, banco de dados e outros recursos de infraestrutura crítica são concedidos exclusivamente pela Raízen aos colaboradores do fornecedor.

Todos os acessos mencionados acima deverão possuir dupla custódia, revisão periódica, monitoramento, sendo que os respectivos registros deverão ser mantidos como evidência da realização desses processos a ser fornecida a Raízen, mediante solicitação formal.

Adicionalmente, o fornecedor deve implementar os seguintes mecanismos mínimos de proteção, e devidamente configurados, atualizados e gerenciados:

a) Antivírus e produtos de gerenciamento de segurança nas máquinas (servidores e estações de trabalho);
b) Proteção de tela por inatividade;
c) Bloqueio da liberação de compartilhamentos administrativos (acesso de administrador local);
d) Bloqueio da adição de contas de administração no grupo administrador local, assim como renomeação e troca de senha;
e) Restrição e monitoramento das portas USB, incluindo o uso de modems e dispositivos de cópia/ armazenamento;
f) Administração de sistema operacional deve ser realizada somente por colaboradores e/ou terceiros devidamente credenciados e capacitados para aquela função;
g) Download e upload de dados, informações e softwares da Internet devem ser evitados e monitorados;
h) Procedimento, processo e controle de aquisição de software e seu licenciamento deve ser formalizado e monitorado de forma a garantir a não utilização de softwares não autorizados;
i) Procedimento, processo para controle e monitoramento de versionamento, atualização e manutenção de software;
j) Procedimento formal, controle e monitoramento de uso de equipamentos pessoais na rede da empresa;
k) Procedimento formal, controle, revisão e monitoramento para acesso remoto, considerando fatores de autenticação forte e mecanismos de criptografia atualizados na conexão e transferência dos dados e informações;
l) Procedimento, processos e ferramentas que viabilizem a consulta e/ou a manutenção do inventário de hardware e software (sistemas desenvolvidos ou adquiridos) ;
m) Caso a contratada decida por infraestrutura ou plataforma como serviço (“as a service”), o provedor deste serviço deve possuir a certificação ISO 27001 e ISAE 3402 tipos 1 e 2 dentro da validade e que cubra os serviços contratos;
n) Quando o objeto da contratação for suporte de TI, administração de sistemas e/ou infraestrutura de TI, plataforma de software em nuvem (software “as a service”), a contratada deve possuir a certificação ISO 27001 e ISAE 3402 tipos 1 e 2 (recomendável), dentro da validade ou possuir a governança de segurança da informação especificada neste documento.

2.3 SEGURANÇA EM RECURSOS HUMANOS

O fornecedor deve assegurar que seus colaboradores entendam suas responsabilidades e estejam em conformidade com os papéis para os quais foram contratados. Estes papéis devem ser definidos, revisados e atualizados periodicamente para que possam ser utilizados como referência para a concessão de acessos.

A contratada deve garantir que seus colaboradores assinem termo de confidencialidade e privacidade de dados com validade mesmo após o desligamento.

A contratada deve garantir que seus colaboradores assinem termo de segurança da informação no trabalho remoto.

2.4 CONTROLE DE ACESSO

O fornecedor deve possuir procedimento, processo e controle formal de registro e cancelamento de usuário para permitir atribuição de direitos de acesso, de acordo com os papéis e responsabilidades dos colaboradores e demais pessoas envolvidas.

Os acessos devem ser concedidos mediante fluxo formal, contemplando o registro e a aprovação de acordo com a criticidade de cada ativo de informação (por exemplo: sistema, aplicação, banco de dados, diretórios de rede e acessos privilegiados).

O monitoramento dos acessos críticos e privilegiados deve ser registrado e mantido como evidência para a conformidade do processo e futuras auditorias.

2.5 SEGURANÇA FÍSICA E LÓGICA

O fornecedor deve efetuar a gestão de acesso físico e lógico para impedir e/ou prevenir o acesso não autorizado, dano e interferências (perdas, furto ou roubo) aos ativos de informação que possam afetar as operações.

O acesso físico ao data center, incluindo data centers terceirizados, deverá assegurar que os fornecedores e administradores desses locais possuam controles de acesso físico e lógico implantados de forma a prevenir os eventos indicados acima. Este acesso deve ser coerente com os papéis e responsabilidades dos colaboradores e devidamente registrados, autorizados e revisados por seus gestores.

Para os serviços relacionados à atendimento ao cliente (call center, cobrança, suporte comercial, entre outros), o ambiente deve ser segregado mantendo os colaboradores que prestam serviços a Raízen apartados fisicamente dos demais ambientes, e alinhados a um procedimento de mesa limpa que assegure que informações da Raízen não fiquem expostas ou sejam acessíveis para terceiros não-autorizados (restrição do uso de celular, impressão de documentos etc.).

2.6 SEGURANÇA DAS OPERAÇÕES E COMUNICAÇÕES

O fornecedor deve efetuar a gestão da operação e ativos de informação (recursos de processamento e armazenamento) que a suporta, de maneira a assegurar que as informações e os recursos estejam protegidos contra ameaças (códigos maliciosos), vazamento e/ou perda de dados e de rastreabilidade (falha no registro de eventos e evidências).

O fornecedor deve assegurar que as informações armazenadas estejam disponíveis para que sejam manipuladas ou recuperadas sempre que solicitado, e que possam ser acessadas e consultadas pela Raízen, quando aplicável.

Além disso, o fornecedor deve assegurar a proteção das informações em redes e recursos de processamento quando transferida dentro da organização e com entidades externas.

Adicionalmente, o fornecedor deve implantar os seguintes mecanismos mínimos de proteção, devidamente configurados e gerenciados:

- Padrões, processos e/ou ferramentas utilizadas para detectar ataque em sistema de rede (Network IDS, Firewall, WAF, anti-DDoS) ;
- Ferramentas e solução contra vazamento de dados e informações (ex.: ferramentas de DLP - data loss prevention) ;
- Solução implementada e configurada para monitoramento de e-mails (ex.: anti-spam, anti-phishing);
- Política formal de webmail ao sistema de correio eletrônico, incluindo monitoramento quando o uso é permitido;
- Software de criptografia de e-mails enviados para internet;
- Solução e ferramentas de criptografia das informações armazenadas de forma que elas somente possam ser acessadas pela Raízen ou terceiros autorizados pela contratante;
- Backup efetuando a gravação de todos os tipos de mensagens das caixas de e-mail (enviadas, recebidas, excluídas) ;

- Procedimento, processo e controle de backups, incluindo tratamento de jobs de backup que falham e teste de recuperação periódico de cópias de segurança;
- Permissão de acesso e monitoramento do e-mail pessoal através da internet da empresa;
- Procedimento, processo e controle para descarte de ativos de informações (papel, disco rígido, dispositivos de armazenamento de dados).

2.7 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

2.7.1 Desenvolvimento Seguro

O fornecedor deve possuir um processo de desenvolvimento seguro como parte integrada do ciclo de vida do desenvolvimento do software. Adicionalmente, ele deve possuir um ambiente produtivo, segregado de forma física e lógica, do ambiente de testes/desenvolvimento.

Em relação aos itens de desenvolvimento seguro, o fornecedor deverá seguir algum framework de desenvolvimento seguro ou entidade de mercado reconhecidos.

O fornecedor deverá possuir procedimento, processo e controle formal de Gestão de mudanças que garanta todo o ciclo de vida do processo.

O fornecedor é responsável por executar uma análise de segurança na aplicação/ serviço/ software, por acompanhar as vulnerabilidades e corrigir os apontamentos identificados, antes de promover novas versões em ambiente produtivo. Caso o fornecedor não execute a análise, ele deverá permitir a execução da avaliação pela equipe da Raízen e posteriormente deverá priorizar as vulnerabilidades identificadas.

2.7.2 Monitoramento da Infraestrutura

O fornecedor deve fornecer ferramentas para consulta da disponibilidade, saúde e desempenho do serviço/ infraestrutura contratada e preferencialmente dispor de comunicação via SNMP ou API para encaminhamento dos eventos e status para as consoles de gerenciamento de serviços e disponibilidade utilizadas pela Raízen.

Declarar a agenda de manutenções programadas (paradas físicas ou atualizações de software) que possam causar parada completa ou parcial do ambiente/serviço contratado.

Além disso, o fornecedor deve dispor de um catálogo de serviços além de mantê-lo atualizado e sempre que possível informar (por e-mail, workshops, treinamentos etc.) sobre os novos serviços ofertados, para que a Raízen fique ciente dos novos serviços.

Quando possível, o fornecedor deve disponibilizar opções de armazenamento das informações, incluindo opções de baixo custo (mas que atendam aos requisitos de segurança), para retenção das informações a longo prazo.

2.7.3 Computação na Nuvem

Caso o fornecedor seja um provedor de serviços de computação em nuvem (IaaS, PaaS ou SaaS), ou faça uso de tecnologia de computação em nuvem como parte da prestação dos serviços para a Raízen, os controles adicionais devem ser implementados:

- Conexão ao ambiente para o provisionamento, orquestração e automação de novos serviços ou infraestrutura através de APIs que serão utilizadas por soluções de gerenciamento de computação em nuvem hibrida (pública e privada) disponíveis no mercado.
- Os dados sensíveis e/ou confidenciais devem ser transmitidos, registrados e/ou armazenados de forma segura entre fornecedores e entre o fornecedor e a Raízen;

- O sistema deve fazer uso de HTTPS em todas as páginas de navegação, porém se em alguma parte não for possível a utilização dele, minimamente deve-se utilizar nas páginas de autenticação;
- Fazer uso de um canal seguro para a troca ou redefinição de chaves criptográficas atualizadas;
- Quando as chaves são armazenadas em seu sistema, elas devem estar adequadamente protegidas e somente acessíveis ao pessoal apropriado em uma base de conhecimento devidamente controlada;
- Os certificados HTTPS devem ser assinados por uma CA confiável. O nome do certificado deve ser igual ao FQDN do site no qual ele será utilizado. O certificado deve ser válido;
- Deve-se impedir que as credenciais de acesso (login e senha) sejam armazenadas diretamente no código do software;
- O processo de redefinição de senha deve ser baseado em questões que são difíceis de adivinhar por meio de força bruta. A mensagem de erro não deve expressar nenhuma informação relevante da conta;
- Suportar múltiplos métodos de autenticação de usuários, como tokens, OTPs via SMS e similares;
- Estabelecer procedimento para federação (via SAML ou qualquer integração com diretórios sob premissas) com redes corporativas;
- SLA de disponibilidade, de atendimento e endereçamento de chamados, política de continuidade/ resiliência/ recuperação de desastres, redundância de infraestrutura e plataforma, política de backup, direito de auditar periodicamente;
- Armazenamento das informações da Raízen de forma segregada e exclusiva;
- Indicar país e região do armazenamento/ processamento de dados no Brasil ou em países/ regiões onde o Brasil possui convênio de colaboração com entidades reguladoras;
- Políticas de acesso com logs e definição de perfis (RBAC) ;
- Trilhas de auditoria (criação, exclusão, manutenção, alteração) de perfis de acesso e outras funcionalidades do sistema;
- O fornecedor deve concordar com a realização de testes de intrusão (EHT-Ethical Hacking Test) em seu ambiente pela Raízen, previamente avisado;
- O fornecedor deve manter atualizado o ambiente onde os serviços são disponibilizados (aplicável para contratação SaaS, PaaS e IaaS). Quando solicitado, as evidências devem ser geradas e apresentadas para a avaliação da Raízen).

2.8 GESTÃO DE INCIDENTES

O fornecedor deve efetuar a gestão de incidentes para assegurar um processo efetivo na atuação de pessoal treinado e equipado para detectar, relatar e tratar fragilidades e eventos de segurança da informação.

É necessário a presença de monitoramento e resposta tempestiva para retomada da disponibilidade do serviço com menor impacto ao negócio, como por exemplo, o uso de serviços de segurança gerenciados.

Caso o fornecedor tome conhecimento ou possua suspeita da ocorrência de um evento ou incidente envolvendo informações ou ativos de informação da Raízen, o fornecedor deverá comunicar imediatamente à área Segurança da Informação e manter a área gestora do contrato informada. Além disso, o fornecedor deve possuir procedimentos para identificação, tratamento, monitoramento e reporte do incidente.

2.9 GESTÃO DA CONTINUIDADE DO NEGÓCIO E RECUPERAÇÃO DE DESASTRES

O fornecedor deve possuir um processo para a gestão de continuidade de negócios e considerar os aspectos de segurança da informação para assegurar a disponibilidade dos recursos de processamento da informação.

O fornecedor deve possuir plano de recuperação em caso de desastres, que descreva o RPO e RTO, SLAs aplicáveis, bem como estratégia para a continuidade das operações/serviços contratados e, divulgar para a Raízen. O prazo do plano de recuperação para serviços críticos (autorização, processamento, atendimento) deve estar adequado a estratégia definida pela Raízen.

Os testes de continuidade deverão ser realizados com periodicidade mínima anual e comunicados previamente a Raízen e os resultados e processos verificados deverão ser compartilhados.

Eventuais impactos na disponibilidade ou qualidade do fornecimento, necessitam ser imediatamente comunicados a Raízen.

2.9.1 Governança

Toda e qualquer alteração nos ambientes utilizados pela Raízen que impacte sua disponibilidade deve ser comunicada por escrito pela área responsável pelo ambiente, com antecedência e deve ser reversível.

O fornecedor deve informar o EoL (End Of Life) e o EoS (End of Support) dos Ativos de Informação e Sistemas periodicamente por escrito e com antecedência, quando aplicável.

Deve atender à exigência regulamentar para que o dado armazenado esteja sempre disponível para que seja manipulado ou recuperado pela Raízen, atendendo desta maneira, às solicitações de órgãos reguladores.

2.10 MIGRAÇÃO E EXPURGO DAS INFORMAÇÕES

Na situação de encerramento de contrato, independentemente da parte solicitante do distrato, o fornecedor deve garantir que todos os dados (por exemplo: arquivos, dados e informações da Raízen, backups e arquivos de recuperação em casos de incidentes, on premise ou nuvem) sejam completamente migrados para o ambiente da Raízen e, posteriormente expurgados de sua propriedade exclusiva, com o acompanhamento dos representantes a serem devidamente informados pela Raízen, utilizando ferramentas que garantam que as informações foram permanentemente deletadas, exemplo WIPE.

Quando, por força de Lei, não for possível realizar o expurgo de dados, o fornecedor deve garantir que os dados estejam protegidos contra vazamento e/ou acesso não autorizado.

Quando se tratar de dados sensíveis – classificados pela Raízen – e, na impossibilidade de acompanhamento do processo pela Raízen, o fornecedor deverá apresentar um laudo sobre o processo de expurgo, emitido por uma consultoria a ser contratada pela área contratante.

2.11 ANÁLISE E AVALIAÇÃO DE VULNERABILIDADES

O fornecedor deve possuir processo formal para a realização de testes de vulnerabilidades e intrusão em seus dispositivos de rede, telecomunicações, aplicações, estações de trabalho e servidores, de maneira periódica e manter os relatórios, assim como resultados e respectivos planos de ação para mitigação e gestão dos riscos, disponíveis para apresentação a Raízen sempre que solicitado.

2.12 SUBCONTRATAÇÃO DE SERVIÇOS PELO FORNECEDOR

Caso o fornecedor subcontrate outro prestador de serviço para realizar as atividades ou processamento/ armazenamento de informações referentes ao contrato, deve informar a Raízen e garantir que seu prestador siga todos os mesmos requisitos de segurança da informação apresentados neste documento, bem como, possibilitar avaliações da Raízen em seu ambiente para verificação dos controles de segurança da informação.

3 CONFORMIDADE

O fornecedor deverá assegurar que a segurança da informação seja implantada e operada em conformidade com as políticas e procedimentos da organização, de maneira a evitar quaisquer violações de obrigações legais, estatutárias, regulamentares ou contratuais relacionadas à segurança da informação e de quaisquer requisitos de segurança que afetem a Raízen.

4 AVALIAÇÃO DE SEGURANÇA DA INFORMAÇÃO EM FORNECEDORES

A área de Segurança da informação da Raízen estabelece o seu processo de avaliação periódica de controles e riscos nos ambientes dos fornecedores, com base nas informações obtidas com a área contratante e com o fornecedor.

Para que a Raízen realize este processo de avaliação, o fornecedor deve atender à solicitação de avaliação feita pelo gestor do contrato ou seu representante, e cumprir os prazos estabelecidos para as etapas de:

a) Preenchimento do questionário de avaliação dos controles de segurança da informação do fornecedor;
b) Agendamento da visita técnica no local de prestação/fornecimento dos serviços, quando aplicável.
c) Elaborar o plano de ação para os itens que apresentarem não conformidade.

É obrigatória a presença de colaboradores do fornecedor que conheçam os aspectos contemplados no questionário durante a visita técnica.

Em caso de identificação de melhorias ou vulnerabilidades no ambiente pela Raízen, o fornecedor deve definir o plano de ação em conjunto com os responsáveis da Raízen. O acompanhamento da evolução dos planos será realizado pelo gestor responsável pela contratação com apoio área de Segurança da Informação.

5 ASPECTOS GERAIS

O fornecedor entende e concorda que este documento pode sofrer atualizações e alterações periódicas. A Raízen comunicará o fornecedor das atualizações e alterações, sendo que o fornecedor deverá se adequar a tais alterações dentro do prazo acordado.

Referidas atualizações e alterações serão acompanhadas nos fóruns de governança internos. O fornecedor deverá fornecer a Raízen evidências das adequações efetuadas, incluindo relatório detalhado e respectivos planos de ação, quando aplicável.