LOJAS RENNER S.A.

RENNER CAMICADO YOUCOM realize ASHUA repassa

Política de Segurança da Informação para Parceiros

Março de 2026

sumário

1 Objetivo

Estabelecer o conjunto de diretrizes de segurança da informação e cibernética a serem implementadas pelos Parceiros[1], quanto à proteção da confidencialidade, integridade e disponibilidade das informações, visando a minimizar as vulnerabilidades e os riscos de segurança para a Lojas Renner S.A. ("LRSA" ou "Companhia"), em linha com as obrigações estabelecidas em contrato, principais recomendações, práticas de mercado e com as regulamentações e controles aplicáveis vigentes.

O estabelecimento de diretrizes e controles aos Parceiros não se limita a esta política, podendo ser definido novos itens e a revisão destes ao longo de toda a relação contratual.

[1] *no contexto deste documento, compreende todas as empresas contratadas pela Lojas Renner S.A.: fornecedores, prestadores de serviços e/ou terceiros, seus sócios e respectivos profissionais, tenham esses profissionais vínculo direto ou indireto com a empresa contratada.*

2 Funções e Responsabilidades

As responsabilidades da Lojas Renner S.A. e do Parceiro devem ser observadas e seguidas, conforme previsto no contrato firmado entre as partes. Cabe ainda ao Parceiro seguir as diretrizes desta política.

3 Diretrizes

- Toda informação criada ou recebida pelo Parceiro, durante o trabalho na Lojas Renner S.A., pertence à LRSA.
- Dados Pessoais devem ser tratados de acordo com as diretrizes previstas na Política de Privacidade disponível nos *sites* das nossas marcas, nas disposições da LGPD (Lei Geral de Proteção de Dados Pessoais – Lei n. 13.709/2018) e demais regulamentações sobre o tema aplicáveis.

- O Parceiro deve zelar pela proteção das informações contra violações de confidencialidade, integridade, disponibilidade.
- As informações da Lojas Renner S.A. devem ser utilizadas com responsabilidade, ética e apenas para os negócios da Companhia, delimitado e estrito ao acordado em contrato entre as partes. O desvio de uso é proibido e terá efeito sobre as penalidades previstas em contrato e legislações vigentes.
- A Lojas Renner S.A. se reserva o direito de monitorar e registrar todo o uso das informações e demais recursos tecnológicos, trafegados, processados ou armazenados no ambiente da LRSA.
- Para implementar sistemas e aplicações, é obrigatório usar ambientes de desenvolvimento, homologação e produção separados. Dados reais, incluindo dados pessoais, devem ser usados somente em ambientes de produção.
- Todo código de desenvolvimento deve estar restrito aos profissionais envolvidos (por exemplo, fábrica de *software*) e equipes da LRSA, com controles de acesso lógico aplicados, por exemplo, mas não limitado ao MFA (Múltiplo Fator de Autenticação).
- É estritamente proibido armazenar, codificar ou embutir (*hard-coded*) senhas, chaves de autenticação, frases secretas ou credenciais de acesso em *scripts*, arquivos de configuração, repositórios proprietários, bibliotecas de terceiros ou em códigos-fontes sob medida ou personalizado, seja em ambiente de desenvolvimento, homologação ou produção.
- É vedado realizar *download* de tabelas de banco de dados de forma parcial ou total, em equipamentos de Parceiros, ainda que em demandas associadas ao trabalho.
- Parceiros que processam, armazenam e/ou transmitem informações de cartões de pagamento (crédito e débito) devem tratá-las como confidenciais e protegidas contra uso indevido, conforme as regras do PCI DSS. Esses ambientes devem considerar segregação adequada, mascaramento de dados, criptografias e controles conforme previsto pelo PCI DSS.

- O Parceiro deve manter processos formais para a identificação, análise e tratamento de vulnerabilidades que possam afetar a segurança da informação, tecnologias e serviços utilizados na prestação das atividades relacionadas à Lojas Renner S.A. Todo Parceiro, com acessos físicos ou lógicos aos ativos de TI, deve ser formalmente identificado, previamente à execução de qualquer atividade nos ambientes da Lojas Renner S.A.
- A Lojas Renner S.A. não se responsabiliza pelo uso indevido, negligente ou imprudente dos recursos e serviços fornecidos aos Parceiros. A Companhia se reserva o direito de analisar dados e evidências para obter provas em investigações e tomar ação em relação às medidas legais e contratuais cabíveis.
- Se por razões tecnológicas ou motivos alheios não for possível seguir as diretrizes desta Política, o Parceiro deve informar imediatamente a área de Segurança da Informação da LRSA.
- Ao término do contrato, o Parceiro deve remover de seus ambientes todos os dados da LRSA, salvo previsão legal, contratual ou aprovação expressa da Lojas Renner S.A. para manutenção de tais dados, especificando-se a justificativa e o tempo de retenção.
- Assegurar a disponibilidade para o atendimento às auditorias e processos de análise de riscos e avaliações de segurança, por parte da Lojas Renner S.A. ou empresa por ela indicada, garantindo a aderência às recomendações e implementações necessárias, dentro dos prazos previamente determinados, conforme venha a ser demandado.

3.1 Uso aceitável das tecnologias

- Os equipamentos, sistemas e recursos tecnológicos, inclusive acessos, disponibilizados aos Parceiros pela LRSA são de propriedade exclusiva da Companhia e devem ser utilizados somente para fins profissionais, relacionados ao desempenho das atividades laborais, conforme previsto em contrato.

- Todos os dispositivos de Parceiros (exemplos: *laptops*, *desktops*, celulares) conectados ao ambiente tecnológico da Lojas Renner S.A. devem seguir às estratégias de proteção definidas pela área de Segurança da Informação da LRSA, incluindo a obrigatoriedade de instalação, ativação e manutenção dos *softwares*, agentes e configurações de segurança determinados pela companhia.
- Caberá ao Parceiro assinar um termo de responsabilidade pelo equipamento da LRSA que ele venha a receber, no ato do recebimento deste, assumindo a responsabilidade e comprometendo-se a mantê-lo em perfeito estado de conservação.
- É explicitamente proibido aos Parceiros o uso de computadores e outros recursos tecnológicos da LRSA incluindo, mas não se limitando às seguintes situações:
    - Utilizar os equipamentos cedidos pela Lojas Renner S.A. para finalidades pessoais ou profissionais alheias às atividades previstas no contrato estabelecido entre as partes.
    - Tentar acessar outro computador, servidor ou rede sem permissão.
    - Burlar sistemas de segurança.
    - Acessar informações confidenciais sem autorização do proprietário.
    - Espionar outras pessoas usando dispositivos eletrônicos ou *softwares*, como *sniffers*.
    - Interromper serviços, servidores ou redes de computadores de qualquer forma.
    - Usar tecnologia para cometer ou ajudar em violações, assédio sexual, perturbação, manipulação ou violação de direitos autorais ou propriedade intelectual sem autorização legal.
    - Hospedar pornografia, material racista ou qualquer outro conteúdo que viole a lei, é terminantemente proibido e passível de sanções e penalidades previstas em contrato e/ou legislações vigentes.
    - Utilizar *software* sem licença oficial do fabricante e não adquiridos pela Lojas Renner S.A.
- É vedado o uso de equipamentos pessoais para acessar o ambiente da LRSA.

- É vedado o uso de ferramentas de comunicação instantânea como por exemplo, WhatsApp, Telegram, Signal ou similares, para troca de arquivos com informações da Lojas Renner S.A.

3.2 Conscientização e treinamentos sobre segurança da informação

- O Parceiro deve implementar e manter programas contínuos e com atualizações regulares de educação, conscientização e treinamento em segurança da informação, com o objetivo de promover comportamentos seguros, o uso adequado dos recursos tecnológicos e o tratamento correto das informações aos seus profissionais.

3.3 Tratamento de incidentes de segurança da informação

- Constitui incidente de segurança da informação um único ou uma série de eventos de segurança da informação indesejados ou inesperados que têm uma probabilidade significativa de comprometer as operações de negócios e ameaçar a segurança da informação da Lojas Renner S.A., bem como qualquer acesso indevido aos sistemas ou à infraestrutura de tecnologia pertencentes ao Parceiro, que venha a abrigar informações da LRSA.
- O Parceiro deve garantir que incidentes de segurança da informação e cibernética, violações das regras de Política de Segurança da Informação da Lojas Renner S.A. sejam reportadas com a máxima brevidade via *e-mail* csirt@lojasrenner.com.br para o devido registro e acompanhamento da resolução, assim como eventuais reportes tempestivos às entidades reguladoras a serem envolvidas.
- O Parceiro deve conduzir o tratamento de incidentes de segurança de seus ambientes, avaliar o risco, registrar as ações para remediação com os responsáveis e atuar em conjunto com a Segurança da Informação da Lojas Renner S.A., para a resolução do incidente que venha a envolver as informações da LRSA, com transparência, imparcialidade, ética e sigilo.

- O Parceiro deve prover contato (*e-mail* e/ou telefone) para incidentes de segurança, garantindo que o atendimento por esse canal ocorra em regime 24x7.
- A Lojas Renner S.A. poderá notificar casos de violação e/ou riscos de segurança, cabendo ao Parceiro tratar imediatamente e prover a mitigação do risco em até 4 (quatro) horas após a notificação.
- Após o encerramento do incidente de segurança, a área de Segurança da Informação da LRSA deve ser reportada sobre o detalhamento do incidente.

3.4 Segurança de perímetro

- A rede de computadores ou recursos em nuvem (*cloud*) devem estar protegidos em seu perímetro por tecnologias tais como, *firewall*, roteadores, sistemas de detecção e prevenção de intrusões, segmentação de rede, e/ou controles equivalentes.
- A configuração dos controles de perímetro deve ser revisada periodicamente para garantir sua eficácia e conformidade com os requisitos de segurança da informação.

3.5 Controle de acesso lógico

- Todos os profissionais do Parceiro devem ter identificadores exclusivos e acessos distintos às tecnologias disponíveis. Os identificadores e senhas devem obedecer a padrões e critérios mínimos conforme melhores práticas vigentes de mercado, como por exemplo, definir senhas fortes como meio de validação de sua identidade quando dos acessos a estação de trabalho, redes, sistemas, servidores e outros ativos de tecnologia, assim como fazer uso obrigatório de MFA (Múltiplo Fator de Autenticação).
- Deve existir um controle de acesso sistemático de forma a garantir que somente as pessoas autorizadas tenham acesso aos sistemas, ativos, servidores e às informações devidamente autorizadas e pré-autorizadas pelo superior responsável do Parceiro.

- Cada usuário deve possuir uma única conta (*login*) pessoal e intransferível, conforme o perfil de acesso definido, devendo os usuários serem identificados e registrados nos acessos aos recursos de informática. O compartilhamento de *login* e senha é proibido.
- O Parceiro deve prover a rastreabilidade de toda autenticação realizada pelo período mínimo de 6 (seis) meses.
- É responsabilidade do Parceiro informar em até 24 horas sobre o desligamento de qualquer membro de sua equipe de trabalho que tenha acesso lógico aos ambientes tecnológicos da Lojas Renner S.A. No caso de membros que tenham acessos de super usuários, acessos a banco de dados ou a códigos de desenvolvimento, esse tempo cai para até 2 horas para notificação. Essa comunicação deve ser feita para o gestor da LRSA responsável pelo contrato, que deverá prover o bloqueio da matrícula na ferramenta de identidades.

3.6 Classificação da informação

- Toda e qualquer informação sobre a Lojas Renner S.A. ou relativa a titulares de dados pessoais devem ser devidamente classificadas e rotuladas obedecendo um padrão mínimo de rotulagem (por exemplo, mas não limitado a: “Público”, “Interno”, “Confidencial”, “Externo” etc.).

3.7 Compartilhamento de informações

- Devem ser implementadas medidas e controles técnicos e administrativos para assegurar que informações, incluindo dados pessoais, trafeguem por redes de transmissão de forma segura e sem comprometimento até os destinatários pretendidos e autorizados, garantindo que apenas estes tenham acesso aos dados.
- Informações, incluindo dados pessoais, só devem ser compartilhadas com quem realmente tenha necessidade delas e quando houver autorização para o compartilhamento dessas informações.

- Antes de compartilhar informações da Lojas Renner S.A, incluindo dados pessoais com outros terceiros, ainda que considerando a possibilidade de cenário previsto em contrato entre as partes envolvidas, é necessário garantir que eles estejam igualmente homologados em Segurança da Informação e Proteção de Dados, conforme o caso e de acordo com normas, leis e/ou regulações vigentes.

3.8 Armazenamento e descarte de informações

- Com o objetivo de garantir a segurança da informação de propriedade da Lojas Renner S.A., bem como a proteção de dados pessoais tratados pela Companhia, todas as informações e dados pessoais devem estar sob regras rígidas e controles criteriosos de armazenamento (*backup* e *restore*), processamento e descarte, de forma que somente as informações estritamente necessárias e permitidas por lei sejam armazenadas pelo período mínimo necessário, ou por força de lei ou regulamento, sendo descartadas de forma segura e definitiva imediatamente após não haver mais necessidade ou uma justificativa de negócio ou, ainda, finalidade legítima para sua manutenção.

3.9 *Logs* e trilhas de auditoria

- Todos os sistemas, dispositivos, servidores e ativos críticos devem ser monitorados por tecnologias apropriadas, como detecção e resposta de *endpoints,* sistemas de detecção e prevenção de intrusões, ferramentas de monitoramento de rede e concentradores de *logs*.
- Os eventos relevantes de segurança nos ambientes do Parceiro devem ser registrados, armazenados e protegidos contra alterações não autorizadas, conforme os requisitos legais e regulatórios aplicáveis.
- O Parceiro deve ser responsável pela gestão dos registros, análise dos eventos e coordenação dos testes em seus ambientes, garantindo que ações corretivas sejam aplicadas quando necessário.

- Os registros de *logs* devem ser mantidos por um período mínimo definido pela legislação vigente ou por exigência contratual, garantindo sua integridade e disponibilidade para auditorias e investigações. Os *logs* devem registrar o acesso a dados pessoais, incluindo por quem, quando e eventuais alterações realizadas. No caso de *logs* que contenham dados pessoais, é necessária a implementação de medidas suficientes para a proteção dos dados pessoais, como controles de acesso, e a observância dos prazos de retenção e exclusão, conforme normas aplicáveis.

3.10 Gestão da cadeia de suprimentos

- O Parceiro deve adotar todas as medidas necessárias para assegurar a aderência dos seus fornecedores que tenham algum relacionamento com os trabalhos executados para a Lojas Renner S.A., a todas as cláusulas contratuais, políticas e outras diretrizes de segurança estabelecidas ao longo de toda relação contratual firmada entre Parceiro e LRSA.

4. Penalidades

- A Lojas Renner S.A. estabelece que o descumprimento das diretrizes da Política de Segurança da Informação para Parceiros está sujeito à aplicação de penalidades, conforme a gravidade da infração e os critérios legais e internos vigentes.
- Caso seja identificada uma conduta não aderente a esta política ou o seu descumprimento, a Lojas Renner S.A. adotará as medidas legais, contratuais, tecnológicas, judiciais ou disciplinares cabíveis.

5. Disposições finais

Esta política entra em vigor a contar da data da sua publicação. No caso de dúvidas, entrar em contato via *e-mail* com:

- **Segurança da Informação:** seguranca_informacao@lojasrenner.com.br.

Exceções a esta política serão submetidas e validadas pela área de Segurança da Informação.

A presente política deve ser revisada no mínimo anualmente ou quando mudanças significativas ocorrerem, de maneira que reflita as novas necessidades para segurança da informação.

LOJAS RENNER S.A.

RENNER CAMICADO YOUCOM realize ASHUA repassa