POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Documento: versão 2024
Data aprovação: 01/07/2024
Vigência: julho/2025

Russell Bedford
taking you further

SUMÁRIO

INTRODUÇÃO

A Política de Segurança da Informação, também conhecida como PSI, é o um conjunto de documentos que orienta e estabelece as diretrizes que a Russell Bedford Brasil utiliza para proteger suas informações, ambientes e imagem.

OBJETIVO

Estabelecer os conceitos e diretrizes de segurança da informação, visando proteger as informações da Russell Bedford Brasil – sócios, colaboradores e dependentes, fornecedores e funcionários, prestadores de serviço, clientes e funcionários, potenciais clientes, candidatos, beneficiários e terceiros.

Este manual é um documento estratégico, com vistas a promover à utilização segura dos ativos de informação da Russell Bedford Brasil, preservando a confiabilidade, a integridade, a legalidade e a disponibilidade das informações para resolução de incidentes e deliberação de procedimentos a serem adotados.

Assim, tem-se como declaração formal da Diretoria acerca de seu compromisso com a proteção de dados pessoais de sua propriedade e/ou sob sua custódia, devendo ser observada por todos os colaboradores internos e externos da Russell Bedford Brasil.

ABRANGÊNCIA

A PSI deve ser de conhecimento de todos os colaboradores da Russell Bedford Brasil, além de parceiros, terceiros e demais pessoas externas que tenham acesso a qualquer informação sensível, ou ao ambiente da empresa.

ORIENTAÇÕES DA POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

4.1 Organização da PSI

Essa Política será a principal referência para as diretrizes de alto nível de Segurança da Informação da Russell Bedford Brasil, outros documentos complementares podem auxiliara detalhar alguns temas:

- **Normas:** as Normas complementares estabelecem regras específicas para serem adotadas em diferentes situações e atividades. Ex.: norma para classificação de informações, norma para cópias de segurança, norma para acesso remoto, entre outros;
- **Procedimentos:** os procedimentos definem o passo a passo para a implementação das diretrizes e normas definidas. Ex.: procedimento para atualização de sistemas, procedimento para resposta a incidentes, entre outros.

4.2 Geral

- A PSI deve ser publicada e comunicada a todos os colaboradores, parceiros, terceiros e outras partes interessadas da Russell Bedford Brasil, buscando ser atendida dentro e fora da organização;
- Tanto a PSI quanto suas normas complementares deverão ser revisadas e atualizadas anualmente, ou sempre que houver alguma mudança relevante na organização;
- Deve ser assinado um Acordo de Confidencialidade, ou o contrato assinado com a Russell Bedford Brasil deverá possuir uma Cláusula de Confidencialidade, como condição para que possa ser concedidoo acesso a informações sensíveis ou ao ambiente da organização;
- Durante as fases de contratação de novos colaboradores, deve ser comunicado ao novo colaborador as orientações sobre Segurança da Informação, assim como a existência dessa PSI;
- Todo colaborador, parceiro, terceiro ou parte interessada com acesso aos ativos de informação deve assinar o termo de ciência, indicando que conhecem a PSI, além de se comprometer a cumprir suas orientações;
- As informações e os sistemas utilizados e/ou desenvolvidos pelos usuários são propriedade exclusivas da Russell Bedford Brasil, não podendo ser considerados de uso pessoal;
- O uso das informações e do ambiente devem ser monitorados, e os registros podem servir de evidência para a aplicação de medidas disciplinares;
- Informações confidenciais não devem estar expostas, em papel ou em outras mídias, na estação de trabalho ou em ambientes compartilhados;
- Todo usuário deve manter sua estação de trabalho bloqueada ao se afastar;
- A Russell Bedford Brasil deve conscientizar seus colaboradores, parceiros, terceiros e outras partes interessadas da importância da Segurança da Informação e sua PSI.

4.3 Tratamento da Informação

- Deve existir um processo de classificação da informação, que considere o grau de confidencialidade e criticidade para o negócio;
- Toda informação deve possuir um proprietário, que será responsável por autorizar o acesso as informações sob sua responsabilidade e monitorar sua integridade;
- As informações devem ser protegidas de forma adequada durante todo seu ciclo de vida (criação, uso, armazenamento, transporte e descarte).
- Os dados pessoais e os dados pessoais sensíveis possuem proteção específica quanto ao seu tratamento, conforme previsto na Lei Geral de Proteção de Dados. Logo, é necessário observar quais dados cada setor da empresa tem acesso, bem como delimitar sua finalidade exclusiva, visando a mantê-los seguros:

Dados pessoais e pessoais sensíveis de colaboradores e seus dependentes:

- São cadastrados no sistema *RentSoft* e pontualmente no sistema Questor podendo ser consultados pelos Gestores das áreas do RH e, conforme necessidade de acesso, pelas áreas do Financeiro e Jurídico.
- Os dados repassados são: Nome, endereço, telefone, e-mail, CNH, data de nascimento, local de nascimento, PIS, título de eleitor, certificado de alistamento, RG, CPF, CTPS, estado civil, filiação, existência de dependente, pagamento de pensão judicial, salário, escolaridade, especializações, cargo, departamento, data de admissão, adicionais, horário de trabalho, contribuição sindical, documento de conselho de classe (OAB, CRC), dados de dependente (nome, data de nascimento, CPF, certidão de nascimento, carteira de vacinação, comprovante escolar, gênero, imagem), dados bancários (cartão, agência, conta), dados do cônjuge (nome, documentos, imagem - vídeo), atestado médico, currículo, registro de ponto, termos de responsabilidade para recebimento de equipamentos, diplomas, autodeclaração racial, folha de pagamento, encargos, filiação partidária de auditores, atestado de capacidade técnica, horas trabalhadas, valor gasto com funcionário, valor de produtividade de funcionário, exames médicos, matrícula, local de trabalho, informações prestadas ao comitê de diversidade.
- Os dados são utilizados com a finalidade de elaborar contrato de trabalho; registro na CTPS; efetuar pagamento de salário; informações para órgãos governamentais responsáveis pelo recolhimento de INSS, FGTS e imposto de renda retido na fonte acompanhamento de colaborador, pagamento de benefícios (VT, VR, Comissão), mentoria de colaboradores e sócios, controle de férias, desligamento, inclusão de pagamento em sistema interno, envio de informações para fins de defesa judicial, alterações de contratos sociais, registro para licitação, contato, verificação de cadastro, envio para agência de transporte (compra de passagem), compra de produto, repasse de correspondência, recolhimento de valores sindicais, registro de responsabilidade, envio para administrador de plano de saúde, envio de informação para cliente, defesa judicial, envio de informação para participação em processo judicial, planejamento estratégico, verificação de atividade de T.I., auditoria, envio de informações para auditar eleição.

Dados pessoais e pessoais sensíveis de sócios:

- Os dados tratados são: Nome, RG, título de eleitor, CPF, CTPS, PIS, matrícula, comprovante de reservista, comprovante de endereço, dado dependente (certidão de nascimento, carteira de vacinação), certidão de casamento, nome e CPF de cônjuge, cópia cartão bancário, fotografia, diploma, carteira conselho de classe, especializações, promoções, currículo, empresas que figurou como sócio, telefone, e-mail, condição de saúde, assinatura digital.
- Os dados são utilizados com a finalidade de avaliação de admissão, elaborar contrato, assinatura em contratos, controle de férias, desligamento, pagamento, defesa judicial, alteração de contrato social, registro para licitação, envio de informação para cliente, envio de informação para agência de transporte, compra de produto, registro de responsabilidade, recebimento e envio de correspondência, planejamento estratégico, envio de informações para entidades públicas, verificação de atividades de T.I., contato, envio de informações para rede internacional.

Dados pessoais e pessoais sensíveis de clientes:

- Os dados tratados são: Nome, CPF, CNH, endereço, telefone, empresa empregadora, horas trabalhadas por cliente, faturamento, nacionalidade, estado civil, profissão, endereço eletrônico, produto adquirido, valores pagos, valores de imposto, filiação, dados de processo judicial: informação bancária, informação salarial, CPTS, RG, imagens, laudos médicos, dependentes, dados sensíveis particulares de cada processo(saúde, filiação partidária), cônjuge.
- A finalidade do tratamento dos dados é a confecção e análise dos contratos, defesa judicial, prestação dos serviços contratados, recebimento/envio de correspondência, atendimento e resolução de demandas solicitadas, consolidação de propriedade, perícia, participação em licitação, auditoria, encaminhamento para entidades públicas, faturamento.

Dados pessoais e sensíveis de funcionários de clientes:

- Os dados tratados são: Nome, cargo, telefone, e-mail, CPF, RG, dados bancários, valores recebidos, dados de dependentes (nome, data de nascimento), matrícula, pagamento de imposto, função, setor, empregador, graduação, exames médicos, atestado médico, afastamentos e motivos, filiação, CNH, endereço, CTPS, dados cônjuge (nome e documentos), registro de ponto, cargo, diploma, termos de responsabilidade, qualificação técnica, currículo, ASO.
- Os dados são utilizados com a finalidade de prestação de serviços contratados (auditoria, consultoria, projetos, contato, participação em reunião), envio para autoridade pública, implementação em sistema.

Dados pessoais de prestadores de serviço:

- Os dados tratados são: Nome, RG, dados bancários, escolaridade, endereço, contato, PIS, valor de salário, valor de recolhimento, valores pagos, data de admissão, função, nacionalidade, estado civil, profissão, CPF, endereço eletrônico, telefone, diploma, currículo, certificados, documento de conselho de classe (OAB,CREA, CRC).
- Os dados são utilizados com a finalidade de elaborar contrato, gestão contratual, efetuar pagamento; envio de informações para órgãos governamentais, emissão de comprovante, faturamento, recebimento de produto, contato, participar de licitações, recolhimento tributário, análise de risco, recebimento de correspondência.

Dados pessoais de fornecedores:

- Os dados tratados são: Nome, CPF, RG, data de nascimento, telefone, endereço, histórico de pagamento, dados bancários (cartão, agência, conta).
- Os dados são utilizados com a finalidade de elaborar contrato, gestão contratual, utilização de serviço/produto, pagamento, emissão de nota, faturamento, negociação, verificação de cadastro da empresa, cobrança, análise de risco, compras, manutenção de imóveis, recebimento de correspondência, avaliação de resultado, planejamento estratégico, suporte de sistemas e rede, representação de empresa.

Dados pessoais de funcionários de fornecedor (Petrobrás):

- Os dados tratados são: Nome, matrícula, valor recebido, benefício, dependentes, valores de imposto.
- Os dados são utilizados com a finalidade de verificação de dados das empresas, autoria, avaliação de adimplência de obrigações trabalhistas e previdenciárias.

Dados pessoais de potenciais clientes:

- Os dados tratados são: Nome, e-mail, telefone, empresa e cargo.
- Os dados são utilizados com a finalidade de estabelecer contato e pesquisar de empresas para oferta e venda de serviços, venda de produto, disparo de e-mail marketing, captação de cliente, envio de informações e propostas.

Dados pessoais de candidatos:

- Os dados tratados são: Nome, e-mail, telefone, empresa e cargo.
- Os dados são utilizados com a finalidade de estabelecer contato e pesquisar de empresas para oferta e venda de serviços, venda de produto, disparo de e-mail marketing, captação de cliente, envio de informações e propostas.

Dados pessoais de beneficiários (projeto PPA):

- Os dados tratados são: Nome, endereço, telefone, e-mail, pagador de benefício, renda, faixa de recebimento de benefício, holerite, IR, fotografia.
- Os dados são utilizados com a finalidade de avaliar e validar renda, autoria, disponibilizar benefício, envio de informações para empresa responsável.

Dados pessoais de terceiros participantes de processo judicial:

- Os dados tratados são: Nome, CPF, estado civil, endereço, documento de identificação (RG, OAB, CREA), matrícula.
- Os dados são utilizados com a finalidade de participar de processos judiciais, elaborar defesa, cálculo, perícia.

Dados pessoais de terceiros de ligações:

- Os dados tratados são: Nome e telefone.
- Os dados são utilizados com a finalidade de controlar, registrar e retornar ligações.

Participantes de evento, projetos, terceiros (público)

- Os dados tratados são: Imagens de terceiros
- Os dados são utilizados com a finalidade marketing, publicações, comunicação de evento, imagens de crianças e/ou adolescentes registrando recebimento de materiais de projeto da comissão de ação social, divulgações internas.

4.4 Gestão de Acesso e Identidades

- O acesso as informações e aos sistemas devem são controlados de acordo com sua classificação, buscando garantir acesso apenas às pessoas autorizadas;
- Os acessos devem ser solicitados e aprovados somente para as informações e sistemas necessários para suas atividades;
- Credenciais de acesso são pessoais e intransferíveis, sendo cada um responsável pela sua e pelas ações realizadas utilizando suas credenciais;
- Sistemas críticos para o negócio devem ser protegidos utilizando múltiplos fatores de autenticação;
- Acessos e credenciais devem ser revisados periodicamente.

4.5 Gestão de Riscos

- Deve existir uma metodologia e um processo para avaliação de riscos;
- Controles de segurança devem ser definidos e aplicados de acordo com a metodologia de avaliação de riscos utilizada.

4.6 Gestão de Incidentes

- Deve existir um processo para o correto tratamento de incidentes de Segurança da Informação, classificando cada incidente de acordo com o impacto na imagem e no negócio da Russell Bedford Brasil;
- Todo incidente que afete a Segurança da Informação deve ser comunicado ao responsável pelo ativo/sistema afetado e ao time de segurança;
- Deve existir um canal de comunicação de incidentes e situações em que a política não esteja sendo seguida.

4.7 Gestão de Cópias de Segurança

- Deve existir uma metodologia e um processo para realização das cópias de segurança;
- Controles de segurança devem ser definidos e aplicados de acordo com a metodologia de avaliação da classificação da informação.

RESPONSABILIDADES

5.1 Colaboradores, parceiros, terceiros e outras partes interessadas

- Cumprir com todas as diretrizes e normas estabelecidas pela Segurança da Informação;
- Estar sempre atualizado e ciente das Políticas, Normas e Procedimentos em uso;
- Utilizar os sistemas corporativos e de produção da empresa, e os recursos a ela relacionados, somente para os fins previstos pela Russell Bedford Brasil;
- Manter sigilo e confidencialidade sobre qualquer informação que possa causar danos a Russell Bedford Brasil, mesmo após o encerramento de suas atividades e relação profissional com a empresa;
- Não discutir assuntos confidenciais da organização em ambientes públicos ou áreas expostas;
- Comunicar a equipe de segurança qualquer violação da política ou incidente de segurança;
- Remover imediatamente documentos que possuam informações confidenciais e privadas de locais públicos, impressoras, máquinas de fax, copiadoras e similares.

5.2 Equipe de Segurança da Informação

- Fornece informações sobre as boas práticas de Segurança da Informação e Privacidade;
- Divulgar a PSI para todos os colaboradores, parceiros, terceiros e outras partes interessadas;
- Colaborar nas atividades de conscientização sobre Segurança da Informação;
- Definir procedimento para configuração segura de equipamentos, ferramentas e sistemas concedidos aos colaboradores, parceiros, terceiros e outras partes;
- Definir procedimentos de monitoramento do ambiente da organização, buscando identificar possíveis incidentes e falhas de segurança, além de gerar indicadores para as atividades da área;
- Realizar auditorias periódicas e avaliações de riscos;
- Definir os procedimentos necessários para o desenvolvimento das atividades.

5.3 Alta direção

- Propor e apoiar iniciativas que visem a segurança da informação e dos ambientes da Russell Bedford Brasil;
- Aprovar e promover as versões da PSI, incluindo suas Normas e Procedimentos;
- Apoiar a conscientização dos colaboradores em relação a relevância da Segurança da Informação, mediante campanhas, palestras, comunicados internos e treinamentos;
- Propor investimentos relacionados à Segurança da Informação com o objetivo de reduzir riscos;
- Propor alterações nas versões da PSI e suas Normas complementares;
- Avaliar e proporações corretivas para incidentes de segurança;
- Definir as medidas cabíveisnos casos de descumprimento da PSI e/ou das Normas complementares.

PENALIDADES

Ao descumprir as diretrizes dessa PSI, ou de suas Normas complementares, você cometerá uma infração funcional, que poderá resultarem advertência, processo administrativo disciplinar ou medidas penais,de acordo com a gravidade do descumprimento e com base nas leis e regulamentações vigentes.

Data da última atualização: 01/08/2024.

contato@russellbedford.com.br

4007-1219

Russell Bedford

taking you further