RELATÓRIO DE IMPACTO

À PROTEÇÃO DE DADOS PESSOAIS

ECSA ENGENHARIA SOCIOAMBIENTAL LTDA

Florianópolis, 06 de julho de 2021

Histórico de Revisões

Data	Versão	Descrição	Autor
06/07/2021	1.0	Conclusão da primeira versão do relatório	Gustavo Silva Rosa

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS - RIPD

OBJETIVO

O Relatório de Impacto à Proteção de Dados Pessoais visa descrever os processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

Referência: Art. 5º, XVII da Lei 13.709/2018 (LGPD).

1 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

Controlador

ECSA ENGENHARIA SOCIOAMBIENTAL LTDA

Operador

ECSA ENGENHARIA SOCIOAMBIENTAL LTDA

Encarregado

GUSTAVO SILVA ROSA

E-mail Encarregado	**Telefone Encarregado**
gustavo@ecsa-sc.com.br	(48) 3371-4704

2 – NECESSIDADE DE ELABORAR O RELATÓRIO

O RIPD da ECSA Engenharia Socioambiental Ltda foi elaborado para os seguintes objetivos:

- para atendimento à Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD) e regulamentação emanadas pela Autoridade Nacional de Proteção de Dados -ANPD.
- para orientação e direcionamento dos funcionários da ECSA Engenharia Socioambiental Ltda com relação ao tratamento das informações pessoais de clientes, colaboradores e demais interlocutores, que por necessidade de negócios são coletadas em seus processos formais.
- para definição de políticas internas de garantia da segurança e governança dos dados pessoais coletados;
- para garantia de proteção e mitigação de riscos eventualmente envolvidos evitando: (i) ameaças ou riscos à privacidade; à segurança; à integridade e/ou à confidencialidade; (ii) destruição acidental ou ilícita; perda; alteração; divulgação ou acesso não autorizado; (iii) quaisquer outras formas ilegais de tratamento; e (iv) incidentes de segurança ou privacidade.

3 – DESCRIÇÃO DO TRATAMENTO

Os sistemas e processos da ECSA Engenharia Socioambiental Ltda foram desenhados para a captação somente dos dados que se fazem pertinentes para a elaboração de contratos comerciais; cadastro de clientes e fornecedores; informações para atendimentos a demandas fiscais e legais; registros de funcionários e para ações de marketing.

3.1 – NATUREZA DO TRATAMENTO

As modalidades de coleta e tratamento de dados pessoais adotadas pela ECSA Engenharia Socioambiental Ltda seguem os seguintes parâmetros:

3.1.1 – Informações para relações comerciais e de negócios

Coleta (o quê?)	Nome completo do representante legal; telefones e endereços de e-mail; números do RG, CPF e CNH.
Coleta (dado sensível?)	Não
Coleta (como?)	Os dados são coletados via cadastro no site para realização de compras, e-mail organizacional ou contato telefônico por nossos colaboradores internos.
Coleta (ciente?)	Em todas as solicitações e demandas de informações: clientes, fornecedores e parceiros são informados e manifestam consentimento livre com relação aos dados informados.
Processamento (como?)	Os dados são utilizados única e exclusivamente para o estrito cumprimento das vendas pelo site, suporte de venda, relações comerciais, como elaboração de contratos comerciais, o acompanhamento do histórico de atendimentos e para os registros legais, entre eles fiscais.
Processamento (onde?)	Os dados coletados são registrados diretamente nos sistemas organizacionais: que fazem o gerenciamento e processamento interno das informações.
Armazenamento (onde?)	Os dados são armazenados diretamente no servidor local da organização e transferidos automaticamente para o servidor gerenciado pela Microsoft como ação de garantia de proteção dos dados.
Compartilhamento	Os dados são compartilhados internamente para o bom andamento dos processos, ou entre as partes para o fortalecimento dos negócios; ou com o departamento jurídico e contábil para o atendimento das partes legais.
Eliminação	Os dados coletados de parceiros e clientes que não foram utilizados para contratos ou para futuros negócios, permanecem registrados nos sistemas, mas tratados como inativos e somente utilizado para controle de eventuais contatos futuros.

3.1.2 – Informações de e-mail marketing e site para contato comercial

Coleta (o quê?)	Nome completo, telefones e endereços de e-mail.
Coleta (dado sensível?)	Não
Coleta (como?)	Os dados são coletados via formulário presente no site ou no e-mail marketing.
Coleta (ciente?)	Ao preencher o formulário o cliente ou interessado manifesta seu consentimento em compartilhar seus dados pessoais e aceita Política de Privacidade disponível no site.
Processamento (como?)	Os dados são utilizados para ações de e-mail marketing com posterior envio de informações a respeito de produtos e contatos telefônicos visando a realização de contatos futuros de vendas e de relações comerciais.
Processamento (onde?)	Os dados registrados no formulário são registrados na plataforma de e-mail, ferramenta Outlook.
Armazenamento (onde?)	Os dados são armazenados diretamente no servidor gerenciado pela Microsoft como ação de garantia de proteção dos dados. A Ferramenta Outlook tem seus dados armazenados no servidor gerenciado pela Microsoft.
Compartilhamento	Os dados são compartilhados internamente para o bom andamento dos processos, ou entre as partes para o fortalecimento dos negócios; ou com o departamento jurídico e contábil para o atendimento das partes legais.
Eliminação	Os dados coletados de parceiros e que não foram utilizados para contratos ou para futuros negócios, permanecem registrados nos sistemas, mas tratados como inativos e somente utilizado para controle de eventuais contatos futuros, sendo eliminados à cada 12 meses se necessário, quando feito a limpeza e tratamento de dados, ou no caso de solicitação de exclusão pelo titular dos dados, desde que inexista obrigação legal por parte do controlador a ser cumprida.

3.1.3 – Informações pessoais para registros e contratos de funcionários

Coleta (o quê?)	Nome completo; telefones; endereços de residência; endereços de e-mail; imagem e dados de CTPS, CNH, RG, CPF; estado civil, nome de filhos, de dependentes legais e nome de cônjuge e escolaridade.
Coleta (dado sensível?)	Origem étnica ou raça; filiação sindical; dados biométricos para utilização no ponto eletrônico e acesso as dependências da empresa; dados relacionados com saúde como exames admissionais, demissionais, periódicos e de saúde.
Coleta (como?)	Os dados são coletados via formulário físico enviados por e-mail ou por acesso telefônico e a ação de preenchimento se dá por consentimento do interessado. Em relação ao dado biométrico o dado é cadastrado diretamente na máquina de ponto eletrônico, ou na máquina de acesso a portaria, fixada internamente para registro de entrada e saída do trabalho.
Coleta (ciente?)	Ao preencher o formulário o funcionário está ciente das informações assinando inclusive um documento de LGPD onde informa-se o tratamento dos dados.
Processamento (como?)	Os dados são utilizados para a confecção de contratos de trabalho, para os registros nos sistemas de folha de pagamento e de benefícios e nos registros legais, como e-social.
Processamento (onde?)	Toda e qualquer informação relativa ao funcionário é armazenada no sistema de folha de pagamento Fortuna.
Armazenamento (onde?)	Os dados digitais são armazenados diretamente no servidor local com sistema de

	backup automático e programado. Os documentos e imagens (cópias de documentos) são arquivados em pasta funcional de acordo com as normas trabalhistas vigentes.
Compartilhamento	Os dados são compartilhados com bancos para processamento de pagamentos de salários; com a operadoras do plano de saúde; vale alimentação e vale refeição; com sindicato para eventuais aditivos e contratos; com e-social para registros legais; com departamento jurídico para elaboração de contratos individuais e coletivos; com o departamento médico para realização de exames periódicos.
Eliminação	Os dados físicos registrados em pasta funcional são eliminados após o período de 5 anos, ficando armazenados em depósito nas dependências da empresa e com controle de acesso.

- Todos os sistemas apontados para o processamento e armazenamento de dados no item 3.1, quando não de propriedade da ECSA Engenharia Socioambiental Ltda, são amparados por contrato de relação comercial e que implica em cláusulas de Proteção de Dados.
- O armazenamento terceiro é protegido por criptografia e segurança garantida pelas empresas de renome internacional;
- O armazenamento local possui acesso de pessoa responsável e com controle de acesso registrado.

3.2 – ESCOPO DO TRATAMENTO

Os dados coletados de acordo com o item 3.1 são para estrito cumprimento de relações comerciais, contratuais e legais, protegidos por cláusulas de sigilo. Todo funcionário da ECSA Engenharia Socioambiental Ltda é treinado e assina termo de ciência com relação as informações.

3.3 – CONTEXTO DO TRATAMENTO

- Qualquer coleta de dados pessoais é avisada ao titular através de documentos informativos no site da ECSA Engenharia Socioambiental Ltda, no contato via e-mail organizacional e por aditivos de contrato, no caso de funcionários;
- A política de sigilo da organização garante ciência por parte de todos os colaboradores do cuidado no trato com as informações pessoais e na proibição de qualquer compartilhamento sem o consentimento pessoal do titular e da organização.
- A ECSA Engenharia Socioambiental Ltda utiliza recursos de segurança robustos para evitar qualquer acesso indevido em sua base de dados.

3.4 – FINALIDADE DO TRATAMENTO

A finalidade para a coleta de dados pessoais pela ECSA Engenharia Socioambiental Ltda atende exclusivamente:

- o cumprimento de obrigação legal fiscal, comercial ou regulatória;
- execução de contrato de compra e venda de mercadorias e outros contratos, assim como de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do

titular dos dados;

- atender aos interesses legítimos para o pleno funcionamento da organização.

Para a elaboração do presente documento foram consultados representantes internos da organização; consultores jurídicos e analistas das empresas que prestam serviços de armazenamento de informações através das ferramentas contratadas, bem como necessidade de consumidores, clientes e prestadores.

4 – PARTES INTERESSADAS CONSULTADAS

Com relação ao atendimento da LGPD e ANPD, foi consultada legislação e materiais que permitam a ECSA Engenharia a garantia de segurança dos dados coletados e o atendimento pleno a legislação; clientes, consumidores e fornecedores para que haja um equilíbrio no atendimento das informações, bem como dos interesses de cada parte envolvida; e os funcionários, a respeito, principalmente, da garantia da segurança de dados sensíveis.

5 – NECESSIDADE E PROPORCIONALIDADE

- A escolha dos dados a serem coletados para implementação dos processos da ECSA Engenharia Socioambiental Ltda foi baseada na preocupação de coletar o mínimo de dados pessoais necessários para execução das suas atividades para elaboração de contratos comerciais e de contratos trabalhistas.
- Internamente, o acesso aos sistemas que gerenciam e armazenam os dados pessoais possui uma política de senha de acesso individualizada.
- Em períodos planejados, a ECSA Engenharia Socioambiental Ltda conduz inspeção sobre as medidas de segurança nas suas plataformas de acesso por profissional credenciado internamente e pelo time de auditores da Microsoft.
- Tanto o sistema de segurança quanto a política de sigilo garantem o correto trato das informações coletadas, sendo possível a aplicação de medidas cabíveis em caso de violações.
- Qualquer violação ou suspeita de violação destas políticas podem ser reportadas diretamente pelo e-mail ecsa@ecsa-sc.com.br.

6 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Para identificação e avaliação de Riscos do Relatório de Impacto à Proteção de Dados Pessoais tratados pela ECSA Engenharia utilizou-se a Matriz Impacto x Probabilidade, como forma de se avaliar o nível dos riscos e descrever medidas, salvaguardas para a mitigação dos mesmos.

Para cada risco identificado, define-se: a probabilidade de ocorrência do evento de risco, o possível impacto caso o risco ocorra, avaliando o nível potencial de risco para cada evento. Para representar os níveis de probabilidade e impacto que, após a multiplicação, resultarão nos níveis

de risco, que direcionarão a aplicação de medidas de segurança utilizou-se os seguintes parâmetros escalares apresentados na tabela a seguir:

Classificação	Valor
Baixo	5
Moderado	10
Alto	15

A figura a seguir apresenta a Matriz Probabilidade x Impacto, instrumento de apoio para a definição dos critérios de classificação do nível de risco, onde o produto da probabilidade pelo impacto de cada risco deve se enquadrar em uma região da matriz apresentada pela Figura 1.

Risco enquadrado na região:

- verde, é entendido como baixo;
- amarelo, representa risco moderado; e
- vermelho, indica risco alto.>

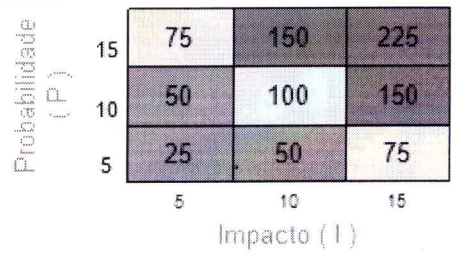

Figura 1: Matriz Probabilidade x Impacto

Tabela de Riscos referentes ao tratamento de dados pessoais pela ECSA Engenharia

Id	Risco referente ao tratamento de dados pessoais	P	I	Nível de Risco (P x I)
R01	Acesso não autorizado.	5	15	75

R02	Modificação não autorizada.	5	15	75
R03	Perda.	5	15	75
R04	Roubo.	5	15	75
R05	Remoção não autorizada.	5	15	75
R06	Coleção excessiva.	5	10	50
R07	Informação insuficiente sobre a finalidade do tratamento.	5	10	50
R08	Tratamento sem consentimento do titular dos dados pessoais (Caso o tratamento não esteja previsto em legislação ou regulação pertinente).	5	15	75
R09	Falha em considerar os direitos do titular dos dados pessoais (Ex.: perda do direito de acesso).	5	15	75
R10	Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais.	5	15	75
R11	Retenção prolongada de dados pessoais sem necessidade.	10	5	50
R12	Vinculação/associação indevida, direta ou indireta, dos dados pessoais ao titular.	5	15	75
R13	Falha/erro de processamento (Ex.: execução de script de banco de dados que atualiza dado pessoal com dado equivocado, ausência de validação dos dados de entrada, etc.).	5	1	75
R14	Reidentificação de dados pseudonimizados.	5	15	75

Legenda: P – Probabilidade; I – Impacto.

[1] Probabilidade: chance de algo acontecer, não importando se definida, medida ou determinada objetiva ou subjetivamente, qualitativa ou quantitativamente, ou se descrita utilizando-se termos gerais ou matemáticos (ISO/IEC 31000:2009, item 2.19).

[2] Impacto: resultado de um evento que afeta os objetivos (ISO/IEC 31000:2009, item 2.18).

[3] Nível de Risco: magnitude de um risco ou combinação de riscos, expressa em termos da combinação das consequências e de suas probabilidades (ISO/IEC 31000:2009, item 2.23 e IN SGD/ME nº 1, de 2019, art. 2º, inciso XIII).

7 – MEDIDAS PARA TRATAR OS RISCOS

Para o tratamento dos riscos apontados no item 6, a ECSA Engenharia adotará as seguintes medidas:

Risco	Medida(s)	Efeito sobre o Risco[1]	Risco Residual[2]			Medida(s)[3] Aprovada(s)
			P	I	Nível (P x I)	

Risco	Medida(s)	Efeito sobre o Risco[1]	Risco Residual[2]			Medida(s)[3] Aprovada(s)
			P	I	Nível (P x I)	
Acesso não identificado, Modificação, Perda, Roubo, Remoção não autorizada.	Implantação de uma política de acesso POP) as informações, intensificando ainda mais o registro do controle, compartilhamento de senhas e reforço no *compliance*.	Evitar	5	15	75	Sim
Coleta, Tratamento e Compartilhamento sem consentimento de usuários	Verificação de todas as formas de coleta de dados de divulgação, via formulário, contratos, e-mails, informando os objetivos da coleta, as formas de tratamento e solicitando o termo de ciência do usuário, que poderá ser o simples resposta ao mesmo.	Aceitar	5	15	75	Sim
Limitação de acesso ao servidor.	Implantar controle de acesso lógico a sala do servidor com registrado de acesso e limitação de acesso.	Evitar	10	5	50	Sim
Limitação, Retenção e eliminação de dados.	Implantação de uma política para coleta mínima de dados, de retenção de dados com prazos determinados e formas claras de eliminação.	Reduzir	10	5	50	Sim

Legenda: P – Probabilidade; I – Impacto. Aplicam-se as mesmas definições de Probabilidade e Impacto da seção 6.

[1] Efeito resultante do tratamento do risco com a aplicação da(s) medida(s) descrita(s) na tabela. As seguintes opções podem ser selecionadas: Reduzir, Evitar, Compartilhar e Aceitar.

[2] Risco residual é o risco que ainda permanece mesmo após a aplicação de medidas para tratar o risco.

[3] Medida aprovada pelo controlador dos dados pessoais. Preencher a coluna com: Sim ou Não.

8 – APROVAÇÃO

ENCARREGADO

GUSTAVO SILVA ROSA

Florianópolis, 06 de julho de 2021.