RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Emitido em: 18/03/2025 às 10:57:17

A seguir reproduzimos todas as informações pertinentes ao tema privacidade e proteção de dados de acordo com os inventários presentes no GPD Governace que deve refletir os apectos atuais escopo da Lei Geral de Proteção de Dados.

Identificação do controlador

CNPJ: 33.054.826/0001-92

Razão Social: Excelsior Seguros – Matriz

Endereço: Marquês de Olinda

Website: https://www.excelsiorseguros.com.br

Área de atuação: Comércio

Tipo de atuação: Privada

Tipo de DPO: Interno

DPO Resposável: Thais Mylane Rangel Souto Maior

Contato do DPO:
thais.rangel@excelsiorsgeuros.com.br

Situação de adequação LGPD

A adequação à LGPD é um processo geralmente longo e quem é melhor executado quando dividido em etapas que se completam e que, não necessariamente são executadas de forma totalmente sequencial.

Atualmente as datas de controle de cada uma dessas etapas de adequação são:

Etapa de Diagnóstico:

Início: Não Informado **Encerramento:** Não Informado **Responsável:** Caroline Monteiro de França

Dados não localizados

Dados não localizados

Parâmetros selecionados para geração deste DPIA

Diretoria: LUCIANO PETRIBU PRESIDÊNCIA **Área:** Auditoria Interna **Departamento:** Não informado

Hipótese: Não informado **Papel:** Não informado **Operador:** Não informado

Ativo: Não informado **Finalidade:** Não informado

Tratamento de dados pessoais

A seguir são listados todos os tratamentos de dados pessoais atualmente em execução pelo controlador suas hipóteses de tratamento previstas na LGPD, seus fundamentos legais em quais ativos de informação esses tratamentos são realizados:

Finalidade: Realização de Testes de Auditoria

Hipótese de tratamento (LGPD): Art. 11º, II a - Obrigação legal ou regulatória

Papel da entidade: Controlador

Trata dados sensíveis? Sim

Trata dados de crianças/adolescentes?: Sim

Origem da Informação: Os dados pessoais utilizados no processo de auditoria interna tem origens diversas, mas são dados que a empresa já possuía para a finalidade do processo que está sendo auditado. Via: E-mail/Teams.

Destino da Informação: Além disso, o relatório pode ser compartilhado com presidência e responsável da área que está sendo auditada. Os dados também podem ser compartilhados com a SUSEP caso solicitado.

Frequência: Muito baixa (> 30 dias de intervalo entre tratamentos)

Volumetria: Alto (1000 - 10000)

Fundamentos Legais

Resolução CNSP nº 416/2021 - Sistema de Controles Internos, a Estrutura de Gestão de Riscos e a atividade de Auditoria Interna

Sobre os dados em tratamento

Artefatos: Apólice

Lista de dados pessoais tratados na finalidade:

- Altura | Sem especialização | Biográfico | Imprescindível para o tratamento? Não
- Beneficiário de seguro | Sem especialização | Biográfico | Imprescindível para o tratamento? Não
- Cargo/função | Sem especialização | Biográfico | Imprescindível para o tratamento? Não
- Código do Corretor na SUSEP | Sem especialização | Cadastral | Imprescindível para o tratamento? Não
- CPF | Sem especialização | Cadastral | Imprescindível para o tratamento? Não
- Data de nascimento | Sem especialização | Biográfico | Imprescindível para o tratamento? Não
- E-mail | Sem especialização | Cadastral | Imprescindível para o tratamento? Não
- Endereço | Sem especialização | Biográfico | Imprescindível para o tratamento? Não
- Faixa salarial | Sem especialização | Biográfico | Imprescindível para o tratamento? Não
- Nome | Sem especialização | Cadastral | Imprescindível para o tratamento? Não
- Número da Apólice | Sem especialização | Cadastral | Imprescindível para o tratamento? Não
- Número da Proposta | Sem especialização | Cadastral | Imprescindível para o tratamento? Não
- Número de telefone | Sem especialização | Biográfico | Imprescindível para o tratamento? Não
- Peso | Sem especialização | Biográfico Sensível | Imprescindível para o tratamento? Não
- Sexo | Sem especialização | Biográfico | Imprescindível para o tratamento? Não

Sobre o processo de consentimento

O tratamento depende de consentimento: Não

Sobre operadores associados

Dados não cadastrado

Sobre o compartilhamento de informações

Os dados são compartilhados? Sim

Como os dados são compartilhados: Além disso, o relatório pode ser compartilhado com presidência e responsável da área que está sendo auditada. Os dados também podem ser compartilhados com a SUSEP caso solicitado.

Com quem os dados são compartilhados

- Microsoft
- Canva Marketing LTDA
- SUSEP

Realiza transferências internacionais ? Não

Sobre o fim do tratamento dos dados

Os dados são descartados? Não **Prazo de armazenamento:** Não Informado

Processo de descarte:

Dados não cadastrado

Sobre os ativos de informação utilizados

Esse tratamento de dados é executado nos seguintes ativos de informação:

Ativos de informação associados ao tratamento de dados

Título do ativo: Sharepoint	**Tipo:** Eletrônico
Título do ativo: Microsoft Teams	**Tipo:** Eletrônico
Título do ativo: E-mail - Outlook	**Tipo:** Eletrônico
Título do ativo: Excel	**Tipo:** Eletrônico
Título do ativo: Canva	**Tipo:** Eletrônico
Título do ativo: Pipe	**Tipo:** Eletrônico
Título do ativo: CoreOn	**Tipo:** Eletrônico

Sobre os riscos associados

Esse tratamento de dados está, atualmente, associado aos seguintes riscos, que serão detalhados em outra seção:

Riscos associados à finalidade de tratamento de dados:

Título do risco: Invasão a rede/sistemas por agentes maliciosos (sistema)

Título do risco: Vazamento de dados pessoais

Medidas administrativas de segurança

A seguir são listadas todas as medidas administrativas (políticas) atualmente em vigor na empresa, onde são documentados os compromissos do controlador com a privacidade dos Titulares de Dados Pessoais:

Política: Política de Privacidade Externa

Tipo da política: Publica
Início de vigência: 02/10/2024 **Fim da vigência:** 31/10/2025
Responsável atual pela política: Thais Mylane Rangel Souto Maior
Tem processo de manutenção? Não **Título do processo de manutenção:** Não Informado

Análise dos parâmetros da política

Integra Governança? Sim **Está completa?** Sim **É exequível?** Sim
Trata o papel do Titular? Sim **Trata o papel do DPO?** Sim **Trata Operadores?** Sim

Abrange o processo de gestão de riscos? Sim
Abrange o processo de gestão de incidentes? Não
Abrange compartilhamento de dados pessoais? Sim

Política: Política de Privacidade Interna

Tipo da política: Interna
Início de vigência: 24/10/2024 **Fim da vigência:** 31/10/2025
Responsável atual pela política: Thais Mylane Rangel Souto Maior
Tem processo de manutenção? Não **Título do processo de manutenção:** Não Informado

Análise dos parâmetros da política

Integra Governança? Sim **Está completa?** Sim **É exequível?** Sim
Trata o papel do Titular? Sim **Trata o papel do DPO?** Sim **Trata Operadores?** Sim

Abrange o processo de gestão de riscos? Sim
Abrange o processo de gestão de incidentes? Não
Abrange compartilhamento de dados pessoais? Sim

Política: Política de Cookies

Tipo da política: Publica
Início de vigência: 21/12/2023 **Fim da vigência:** 19/09/2025
Responsável atual pela política: Thais Mylane Rangel Souto Maior
Tem processo de manutenção? Não **Título do processo de manutenção:** Não Informado

Análise dos parâmetros da política

Integra Governança? Sim **Está completa?** Sim **É exequível?** Sim
Trata o papel do Titular? Sim **Trata o papel do DPO?** Não **Trata Operadores?** Não

Abrange o processo de gestão de riscos? Não
Abrange o processo de gestão de incidentes? Não
Abrange compartilhamento de dados pessoais? Não

Medidas técnicas de segurança

A seguir são listadas todas as medidas técnicas atualmente implementadas em cada ativo da informação utilizado para a realização de rotinas de tratamento de dados pessoais e o nível de Confiabilidade desses ativos e acordo com as atuais medidas técnicas em vigor:

Dados não cadastrado

Gestão de riscos de privacidade e segurança da informação

Para a gestão de riscos de privacidade e segurança da informação, utilizamos a seguinte matriz estruturada para classificação da criticidade de cada risco, que é composta de acordo com a classificação de impacto do risco e sua probabilidade percentual em ocorrer:

		Impacto		
		Baixo	Média	Alto
Probabilidade	100%	Alta	Urgente	Urgente
	90%	Moderada	Urgente	Urgente
	80%	Moderada	Alta	Urgente
	70%	Moderada	Alta	Urgente
	60%	Moderada	Alta	Alta
	50%	Baixa	Alta	Alta
	40%	Baixa	Moderada	Alta
	30%	Baixa	Moderada	Moderada
	20%	Baixa	Baixa	Moderada
	10%	Baixa	Baixa	Moderada

A seguir são listados todos os atuais riscos de privacidade e proteção de dados identificados e que estão sendo gerenciados pelo controlador, ordenados de acordo com sua criticidade:

Risco: Vazamento de dados pessoais

Criticidade: Moderada

Classificação de impacto: Alto

% de probabilidade de ocorrência: 10%

Personas afetadas pelo risco: Controlador

Status atual: Encontrado

Data de registro: 09/01/2025

Data do disparo: Não Informado

Responsável atual pela gestão do risco: Thais Mylane Rangel Souto Maior

Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Mitigar

O que estamos fazendo para tratar o risco:

- Foi implementado controle para mitigação

Ações após disparo:

- ação

Sobre as associações do risco

Processos de negócios associados ao risco:
• Realização de Testes de Auditoria

Tratamento de dados pessoais associados ao risco:
• Realização de Testes de Auditoria

Ativos da informação associados ao risco:
Dados não cadastrado

Risco: Sequestro de dados pessoais - ransonware

Criticidade: Moderada

Classificação de impacto: Alto

% de probabilidade de ocorrência: 10%

Personas afetadas pelo risco: Não Informado

Status atual: Encontrado

Data de registro: 13/03/2025

Data do disparo: Não Informado

Responsável atual pela gestão do risco: Thais Mylane Rangel Souto Maior

Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Mitigar

O que estamos fazendo para tratar o risco:

- O plano de ação para a mitigação do risco de ransonware envolve medidas técnicas e administrativas, como: firewall, antimalware e conscientização dos colaboradores.

Ações após disparo:

- Não Informado

Sobre as associações do risco

Processos de negócios associados ao risco:
Dados não cadastrado

Tratamento de dados pessoais associados ao risco:
Dados não cadastrado

Ativos da informação associados ao risco:
Dados não cadastrado

Risco: Tratamento irregular por desrespeito aos direitos dos titulares

Criticidade: Moderada

Classificação de impacto: Médio

% de probabilidade de ocorrência: 40%

Personas afetadas pelo risco: Não Informado

Status atual: Encontrado

Data de registro: 13/03/2025

Data do disparo: Não Informado

Responsável atual pela gestão do risco: Thais Mylane Rangel Souto Maior

Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Mitigar

O que estamos fazendo para tratar o risco:

- A estratégia para tratar o risco em questão envolve a aplicação de medidas técnicas e administrativas, como: conscientização de colaboradores, anexos contratuais sobre proteção de dados pessoais, DLP, firewall, antimalware, controle de acessos, dentre outras.

Ações após disparo:

- Não Informado

Sobre as associações do risco

Processos de negócios associados ao risco:
Dados não cadastrado

Tratamento de dados pessoais associados ao risco:
Dados não cadastrado

Ativos da informação associados ao risco:
Dados não cadastrado

Risco: Invasão a rede/sistemas por agentes maliciosos (sistema)

Criticidade: Moderada

Classificação de impacto: Alto

% de probabilidade de ocorrência: 30%

Personas afetadas pelo risco: Não Informado

Status atual: Encontrado

Data de registro: 13/03/2025

Data do disparo: Não Informado

Responsável atual pela gestão do risco: Thais Mylane Rangel Souto Maior

Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Mitigar

O que estamos fazendo para tratar o risco:

- A estratégia de tratamento do risco envolve a adoção de diversas medidas técnicas e administrativas, como: firewall, MFA, controle de acessos, antimalware, conscientização dos colaboradores, dentre outras.

Ações após disparo:

- Não Informado

Sobre as associações do risco

Processos de negócios associados ao risco:
• Realização de Testes de Auditoria

Tratamento de dados pessoais associados ao risco:
• Realização de Testes de Auditoria

Ativos da informação associados ao risco:
Dados não cadastrado

Risco: Acessos internos não autorizados

Criticidade: Baixa

Classificação de impacto: Baixo

% de probabilidade de ocorrência: 40%

Personas afetadas pelo risco: Não Informado

Status atual: Encontrado

Data de registro: 13/03/2025

Data do disparo: Não Informado

Responsável atual pela gestão do risco: Thais Mylane Rangel Souto Maior

Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Mitigar

O que estamos fazendo para tratar o risco:

- A estratégia para o risco envolve a adoção de mecanismos de acesso como login e senha, além de múltiplos fatores de autenticação. É necessário ainda implementar medida organizacional que permita maior controle sobre a concessão e a revogação de acessos.

Ações após disparo:

- Não Informado

Sobre as associações do risco

Processos de negócios associados ao risco:
Dados não cadastrado

Tratamento de dados pessoais associados ao risco:
Dados não cadastrado

Ativos da informação associados ao risco:
Dados não cadastrado

Risco: Indisponibilidade das informações (sistema/infra)

Criticidade: Baixa

Classificação de impacto: Médio

% de probabilidade de ocorrência: 10%

Personas afetadas pelo risco: Não Informado

Status atual: Encontrado

Data de registro: 18/03/2025

Data do disparo: Não Informado

Responsável atual pela gestão do risco: Thais Mylane Rangel Souto Maior

Sobre a estratégia de gestão do risco

Estratégia adotada para tratar o risco: Mitigar

O que estamos fazendo para tratar o risco:

- O risco é mitigado tendo em vista o monitoramento contínuo da rede e dos sistemas, além da realização de backups periódicos com vistas a evitar a indisponibilidade das informações.

Ações após disparo:

- Não Informado

Sobre as associações do risco

Processos de negócios associados ao risco:
Dados não cadastrado

Tratamento de dados pessoais associados ao risco:
Dados não cadastrado

Ativos da informação associados ao risco:
Dados não cadastrado