PSM COMPANY

Manual
Sistema de Gestão da Privacidade da Informação
MGPI

ABNT NBR ISO 27701:2022

Sumário

1. Objetivo do SGPI

Fornecer uma estrutura organizacional e procedimentos para garantir o cumprimento das normas de privacidade e proteção de dados pessoais - DP, garantindo que a **PSM Company** os trate DP de forma ética, legal e responsável, protegendo os direitos e privacidade dos titulares de dados, ao mesmo tempo em que promove a conformidade e a confiança do público.

1.1. Documento de referência

- **ISO/IEC 27000** – *Information technology – Security techniques – Information security management systems – Overview and vocabulary*;
- **ISO 27001:2022 –** Segurança da Informação, segurança cibernética e proteção à privacidade – Sistemas de gestão da segurança da informação – Requisitos;
- **ISO 27002:2022 –** Segurança da Informação, segurança cibernética e proteção à privacidade – Controles de segurança da informação;
- **ISO 27701:2020 –** Técnicas de segurança – Extensão da ABNT NBR ISO/IEC27001 e ABNT ISSO/IEC27002 para gestão de privacidade -Requisitos e diretrizes.
- **Lei nº 13.709 de 14 de agosto de 2018** – **L**ei **G**eral de **P**roteção de **DP**;
- **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016** – GDPR.

1.2. Definições

- **SGPI - S**istema de **G**estão da **P**rivacidade da **I**nformação;
- **LGPD -** Lei Geral de Proteção de Dados – no Brasil;
- **GDPR – *G****eneral* ***D****ata* ***P****rotection* ***R****egulation* (em inglês) ou
  Regulamento Geral de Proteção de Dados (em português);
- **PII (DP)** - ***P****ersonally* ***I****dentifiable* ***I****nformation*;
- **DP – D**ados **P**essoais**;**
- **TI** – **T**ecnologia da **I**nformação;
- **SI** – **S**egurança da **I**nformação;
- **PDCA - *P****LAN* – ***D****O* – ***C****HECK* – ***A****CT* (em inglês)
  PLANEJAR – EXECUTAR – CHECAR – AGIR (em português;
- **SWOT** - ***S****trengths,* ***W****eaknesses,* ***O****pportunities e* ***T****hreats* (em inglês) ou
  Forças, Fraquezas, Oportunidades e Ameaças (em português);
- **NC**s - **N**ão **c**onformidade(s);
- **O**Ms - **O**portunidades de **m**elhoria(s).

2. Contextualização

O SGPI da **PSM Company**, se tornou crucial com o aumento das preocupações com a privacidade dos dados em todo o mundo e a implementação de leis rigorosas de proteção de dados, LGPD e GDPR.

O SGPI surgiu de em um cenário onde a coleta, armazenamento e processamento de DP se tornaram essenciais para as operações comerciais, governamentais e sociais. Com o avanço da tecnologia e a proliferação de serviços digitais, enormes volumes de dados são gerados e compartilhados diariamente, o que cria desafios significativos em relação segurança das informações e à privacidade.

O SGPI é uma resposta estratégica e operacional à necessidade crescente de proteger a privacidade e a segurança dos DP em um mundo digital cada vez mais complexo e interconectado. Ele desempenha um papel fundamental na construção da confiança do público, na mitigação de riscos e na promoção de práticas de tratamento de dados éticas e responsáveis.

Nesse contexto, temos:

- **Compliance Legal:** as leis de proteção de dados estabelecem requisitos rigorosos para o tratamento de informações pessoais. O não cumprimento dessas leis pode resultar em multas substanciais e danos à reputação.
- **Expectativas dos Consumidores:** Os consumidores estão cada vez mais conscientes sobre a importância da privacidade e exigem que as empresas protejam seus DP de forma adequada.
- **Riscos de Segurança:** Os DP são alvos frequentes de hackers e cibercriminosos, representando um risco significativo de violações de segurança e vazamentos de informações.
- **Reputação e Confiança:** Incidentes de segurança e violações de dados podem ter um impacto devastador na reputação de uma organização e na confiança do público.
- **Complexidade Tecnológica:** Com a crescente variedade de sistemas e plataformas utilizados pelas organizações, é desafiador garantir uma proteção consistente e eficaz dos DP.

Diante dessas pressões, o SGPI surge como uma abordagem sistemática para lidar com essas questões. Ele envolve a implementação de políticas, procedimentos, controles e tecnologias destinadas a garantir a conformidade com as leis de privacidade, proteger os DP contra ameaças e violações, e promover uma cultura de responsabilidade e transparência em relação ao tratamento de dados.

2.1. Premissas do SGPI

São os princípios fundamentais que norteiam a sua concepção, implementação e operação. Essas premissas são essenciais para garantir que o SGPI atenda aos objetivos de proteção de dados e privacidade da **PSM Company** de forma eficaz e consistente. Algumas das principais premissas de um SGPI incluem:

- **Legalidade e Conformidade:** deve garantir que o tratamento de DP esteja em conformidade com todas as leis, regulamentos e normas aplicáveis relacionadas à privacidade e proteção de dados, incluindo a LGPD - Lei Geral de Proteção de Dados - no Brasil, o GDPR - Regulamento Geral de Proteção de Dados - na União Europeia, entre outros;
- **Transparência e Informação:** deve promover a transparência no tratamento de DP, informando os titulares sobre como seus dados são coletados, usados e protegidos, bem como quais são seus direitos em relação aos seus dados;
- **Princípio da Finalidade:** deve garantir que os DP sejam coletados e tratados para finalidades específicas, legítimas e explícitas, e que não sejam utilizados de forma incompatível com essas finalidades;
- **Minimização de Dados:** deve garantir que apenas os DP necessários para a realização das finalidades pretendidas sejam coletados, e que sejam mantidos apenas pelo tempo necessário para alcançar essas finalidades;
- **Segurança da Informação e privacidade:** deve implementar medidas técnicas e organizacionais adequadas para proteger os DP contra acessos não autorizados, vazamentos, perdas, alterações ou qualquer forma de tratamento inadequado;
- **Responsabilidade e Prestação de Contas:** deve atribuir responsabilidades claras aos envolvidos no tratamento de DP e garantir que todos os processos sejam documentados, monitorados e auditados regularmente para garantir conformidade e transparência;
- **Respeito aos Direitos dos Titulares:** deve garantir que os direitos dos titulares dos dados sejam respeitados e que mecanismos adequados estejam em vigor para permitir que os titulares exerçam seus direitos, como o direito de acesso, retificação, exclusão e portabilidade de seus DP;
- **Melhoria Contínua:** deve ser continuamente revisado, avaliado e aprimorado para garantir sua eficácia e conformidade contínuas com as leis e melhores práticas em proteção de dados e privacidade da informação.

Essas premissas formam a base sobre a qual um SGPI é construído e operado, garantindo que a **PSM Company** esteja em conformidade com as leis de proteção de dados, proteja

os direitos dos titulares de dados e promova uma cultura de respeito segurança da informação e à privacidade.

2.1.1. Metas

Algumas das metas específicas de um SGPI incluem:

- **Cumprimento Legal:** assegurar que a **PSM Company** esteja em conformidade com as leis e regulamentos de privacidade de dados aplicáveis, como a LGPD - Lei Geral de Proteção de Dados, no Brasil;
- **Proteção de Dados:** garantir a proteção adequada dos DP sob a responsabilidade da **PSM Company**, evitando acessos não autorizados, vazamentos ou uso inadequado;
- **Gestão de Riscos:** identificar, avaliar e mitigar os riscos associados ao tratamento de DP, incluindo riscos de segurança da informação e privacidade e privacidade, conformidade legal e danos à reputação;
- **Transparência e Confiança:** promover a transparência no tratamento de DP, informando os titulares sobre como seus dados são coletados, usados e protegidos, contribuindo assim para construir a confiança do público;
- **Eficiência Operacional:** implementar processos eficientes para gerenciar o ciclo de vida dos DP, desde a coleta até a exclusão, garantindo sua precisão, atualização e relevância;
- **Melhoria Contínua:** estabelecer mecanismos de monitoramento e revisão para garantir que o SGPI seja constantemente aprimorado e adaptado às mudanças nos requisitos legais, tecnológicos e organizacionais.

2.2. Perfil

A **PSM Company** atua há mais de 15 anos na contratação e alocação de profissionais para as seguintes atividades:

- Desenvolvimento de sistemas;
- Infraestrutura e servidores;
- Redes e sistemas operacionais;
- Banco de dados;
- Suporte – *Service desk e field service*;
- Processos de negócio;
- Qualidade e testes;
- Segurança da informação e privacidade;
- Aplicações.

2.3. Missão, Visão e Valores

2.3.1. Missão

Oferecer soluções em tecnologia e gestão de Recursos Humanos gerando valor a nossos Clientes

2.3.2. Visão

Sermos reconhecidos como referência na prestação de serviços em tecnologia e gestão de Recursos Humanos

2.3.3. Valores

Acreditamos nas Pessoas e nelas investimos seguindo diretrizes como: Ética, Valorização da Diversidade, Transparência e Companheirismo.

Nota: A missão, a visão e os valores da **PSM Company** estão documentados na Análise do Contexto Organizacional.

3. Política

A Política de Segurança da informação e privacidade é a expressão do compromisso corporativo, validado pela direção, frente às expectativas das partes interessadas no que tange à segurança da informação e privacidade e atendimento aos requisitos legais e outros requisitos.

"Realizar a gestão de serviços de Tecnologia da Informação com o comprometimento de atender os requisitos aplicáveis, proteger e garantir a privacidade de dados e informações pertinentes e promover a melhoria contínua."

4. Escopo

NORMA: NBR ISO/IEC 27701:2019 – Gestão da Privacidade da Informação;

Sistema de Gestão da Privacidade da Informação – SGPI - na prestação de serviços em Tecnologia da Informação com terceirização de profissionais especializados, com o suporte das atividades de Gestão de Pessoas, Recrutamento e Seleção, Administração de Pessoal, Financeira, Faturamento, Novos Negócios e Pós-Venda, Segurança da Informação, como controladora e operadora de dados, conforme DECLARAÇÃO DE APLICABILIDADE - ANEXO A – B, revisão 01 – de 10/06/2024.

Site incluído no escopo:

- PSM Company – Professional Services Management Informática Ltda.
  Rua Luiz Seráphico Junior, 511 – Cj. 181 – Jardim Caravelas – São Paulo/SP

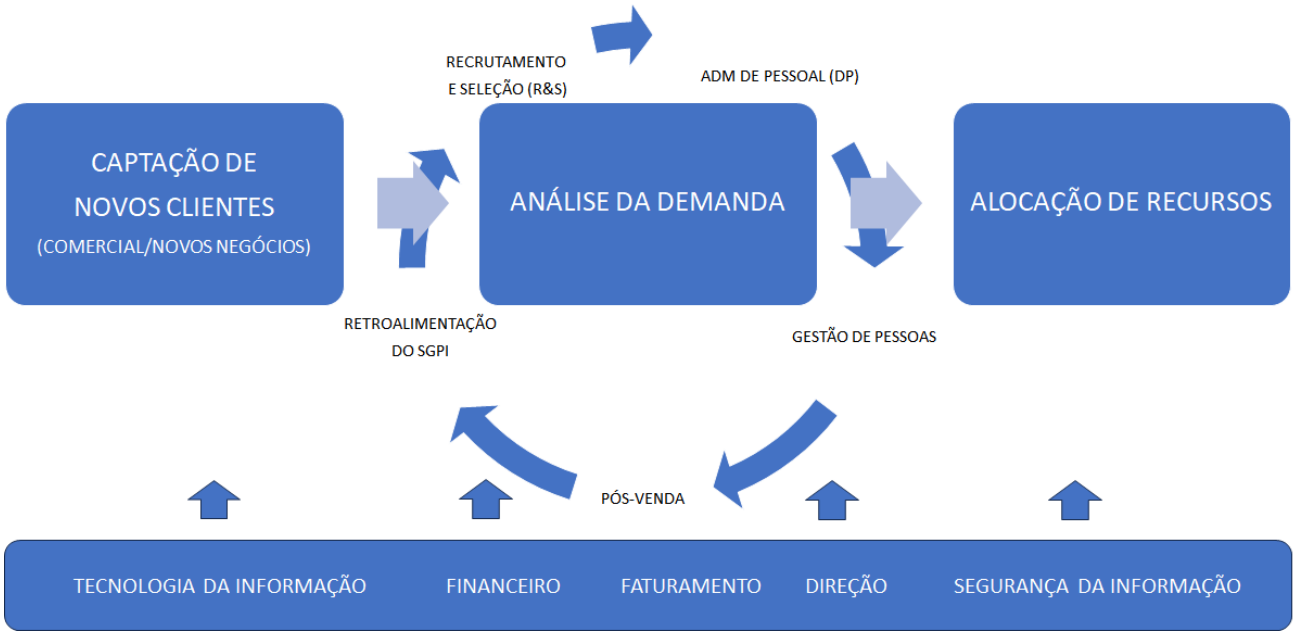
CEP 04729-080

Declaração de Aplicabilidade: DOC-Anexo A_B - Declaração de Aplicabilidade

Nota: O motivo para a tradução do termo "***personally identifiable information - PII***" por dados pessoais - **DP** é o uso corrente da expressão dados pessoais no Brasil e sua adoção pela lei brasileira que trata de privacidade e proteção de dados pessoais - Lei 13.709/2018 – Lei Geral de Proteção de Dados Pessoais – LGPD.

4.1. Interação dos Processos

O processo de oferta de serviços consiste na captação de novos clientes pela área de Novos Negócios, análise da demanda e alocação de recursos, pela área de Recrutamento e Seleção, identificação de eventuais necessidades de treinamento, pela área de Gestão de Pessoas, suporte relacionado às questões de documentação, pela área de Administração de Pessoal e suporte ao cliente pela área de Pós-Venda, contando ainda com o apoio das áreas de TI, SI Financeiro, Faturamento e Direção.



5. Análise de riscos e oportunidades

A **PSM Company** considera estratégicas para o negócio as questões externas e internas que possam resultar em risco ou oportunidade e que afetem ou possam impactar a segurança da informação e privacidade, as partes interessadas e a eficácia do SGPI, com efeitos sob os ativos físicos, financeiros, operacionais, imagem, marca e a sua reputação.

A identificação de riscos e oportunidades pode advir da análise crítica sistêmica, da análise de atendimento aos requisitos legais e outros requisitos, manifestações de partes interessadas, avaliação de riscos, dentre outros.

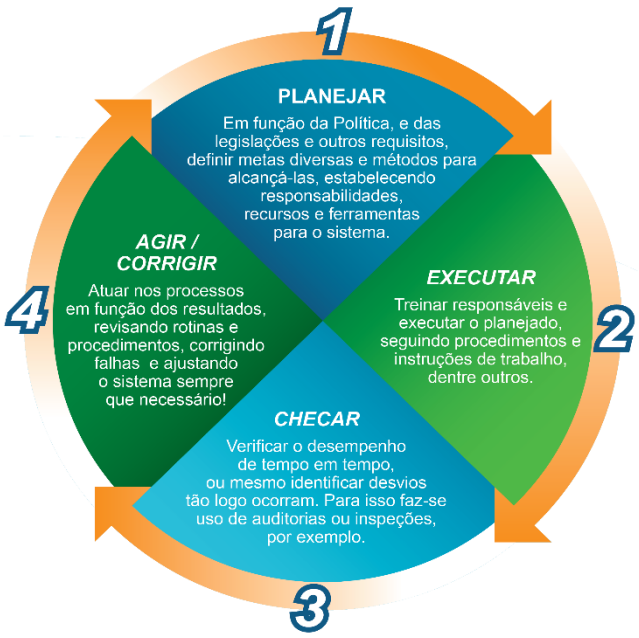
A análise de riscos e oportunidades é realizada por meio da Matriz SWOT.

Os riscos e oportunidades são anualmente avaliados pela direção durante a reunião de análise crítica do sistema de gestão, ou conforme necessidade.

6. Elementos do SGPI

São os componentes fundamentais que constituem a estrutura e operação do sistema - SGPI. Eles são essenciais para garantir que a privacidade dos dados pessoais seja adequadamente protegida e gerenciada dentro da **PSM Company**, seus principais elementos incluem: Política de Privacidade e Proteção de Dados; Atribuição de Responsabilidades; Avaliação de Riscos; Controles de Segurança da Informação; Procedimentos de Coleta e Consentimento; Gestão de Direitos dos Titulares; Treinamento e Conscientização; Monitoramento e Auditoria; Resposta a Incidentes; Melhoria Contínua. Esses elementos formam a estrutura essencial de um SGPI, fornecendo as bases para uma gestão eficaz da privacidade da informação dentro de uma organização, conforme exigido pelas leis e regulamentos de proteção de dados.

O SGPI é um conjunto de processos definidos que permitem que a PSM Company gerencie de forma sistemática suas oportunidades, seus riscos e impactos relacionados à segurança da informação e privacidade. Para tal, é estabelecido um processo sistêmico, refletido em documentos, rotinas de trabalho e registros que visam auxiliar seu melhor desempenho, baseado no ciclo PDCA, para estruturar suas fases e processos. Graficamente, temos:



Este ciclo envolve desde o planejamento de ações à execução, medição do desempenho, correções e melhorias, visando a leitura constante e aperfeiçoamento dos processos, planos de

trabalho e demais elementos que constituem o SGPI. Estabelece, assim, as bases para a melhoria contínua, através de lições aprendidas. Cada uma das etapas do ciclo de gestão do SGPI é descrita nos respectivos procedimentos.

6.1. Ciclo PDCA

6.1.1. Planejar

6.1.1.1. Contexto da Organização

A organização analisa seu contexto e identifica riscos e oportunidades de negócio por meio da Matriz SWOT.

6.1.1.2. Requisitos legais e outros requisitos

A gestão dos requisitos legais promove a aderência do SGPI e dos processos organizacionais ligados ao mesmo frente às exigências de legislações em nível federal, estadual e municipal aplicáveis. Por essa razão, também servem de referência na definição dos elementos do SGPI.

Os monitoramentos associados ao atendimento a requisitos legais são realizados e registrados no REG-SGSI-003 - Requisitos Legais e Outros Requisitos. Sua atualização é realizada periodicamente, com verificação anual.

O monitoramento do atendimento aos requisitos é realizado conforme PROC-SGSI-003 - Requisitos Legais e Outros Requisitos.

6.1.1.3. Partes interessadas

Estão definidas na Análise do Contexto Organizacional.

6.1.1.4. Objetivos, metas e indicadores

Os Objetivos, metas e Indicadores, baseados na Política do SGPI, requisitos legais e outros requisitos, são estabelecidos de modo a promover e estimular um ambiente de melhoria contínua nos processos considerados significativos e críticos. Além disso, são também elaborados com a expectativa de gerar comprometimento da organização e bom desempenho do próprio sistema. Tal processo está definido no PROC-SGSI-002 - Objetivos, Metas e Indicadores.

Os Objetivos, Metas e Indicadores do SGPI, com conteúdo aprovado junto à direção, resumem o conjunto de informações necessárias à gestão e acompanhamento dos indicadores. Os indicadores são gerenciados e registrados pela área de TI.

6.1.1.5. Recursos, funções, responsabilidades, funções e autoridades

O SGPI conta com o apoio das áreas de Gestão de Pessoas e TI para gestão. Entretanto, ressalta-se que a manutenção e contribuição para melhoria contínua do SGPI são atribuições de todos os envolvidos. No conjunto de documentos do SGPI estão descritas as responsabilidades específicas.

6.1.2. Executar

6.1.2.1. Competência, Treinamento, treinamento e conscientização

A **PSM Company** identifica as necessidades de competência, treinamento e conscientização, sendo que o SGPI identifica as necessidades aplicáveis frente aos requisitos legais e normativos, conforme PROC-SGSI-010 - Gestão de Treinamentos, Competências e Conscientização.

Este esforço é complementado com ações de comunicação que visam contextualizar os elementos do SGPI na rotina dos empregados e contratados, bem como sensibilizá-los para a importância de promover a melhoria contínua de processos.

6.1.2.2. Comunicação

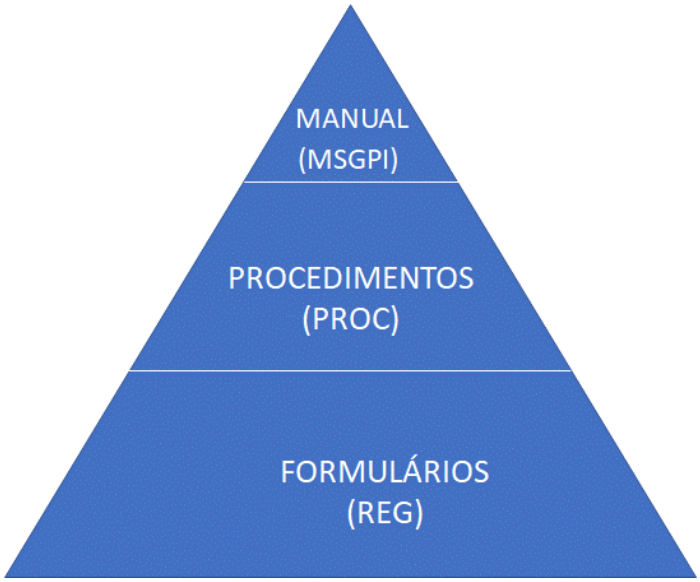
A organização prevê esforços de comunicação no ambiente interno e externo. As comunicações visam gerar atendimento e alinhamentos frente aos elementos do SGPI e/ou identificar expectativas diversas.

No ambiente interno, comunicações visam sensibilizar funcionários e fornecedores para atendimento e contribuição frente aos elementos do SGPI, bem como identificar situações diversas que evidenciem oportunidades de melhoria ou desvios frente ao sistema. A comunicação interna é realizada via e-mail, reuniões e *WhatsApp*.

No ambiente externo, a **PSM Company** disponibiliza website corporativo, onde constam os canais para contato. A sistemática estabelecida para comunicação está descrita no PROC-SGSI-006 - Gestão da Comunicação Interna e Externa.

6.1.2.3. Documentação

Os documentos que estruturam o SGPI, incluindo este Manual, seguem a esquematização abaixo:



Além dos documentos específicos para o sistema de gestão, a PSM Company conta também com Políticas, Normas e Procedimentos que descrevem as estratégias e processos de cada atividade.

Este Manual descreve todos os elementos do SGPI e, sempre que aplicável, direciona à documentação correlata. Toda elaboração, aprovação, distribuição e controle dos documentos e registros associados ao SGPI é tratada no PROC-SGSI-001 - Controle de Informação Documentada. Documentos de origem externa e outros requisitos aplicáveis ao SGPI são também tratados neste mesmo procedimento.

6.1.2.4. Controle Operacional

Em função da identificação de riscos de segurança da informação e privacidade, são estabelecidos e implementados, junto àqueles considerados significativos ou críticos, controles operacionais.

Todos os controles visam garantir o atendimento às premissas da Política de Segurança da informação e Política de Privacidade, requisitos legais e outros requisitos aplicáveis. Ainda, contribuem para a organização dos elementos pertinentes às normas, para evidenciação dos mesmos e suporte à melhoria contínua do SGPI. O acompanhamento é conforme PROC-SGSI-007 - Controle Operacional e Gestão de Riscos. O PROC-SGSI-005 - Gestão de Não Conformidades e Ações de Melhoria prevê ainda o tratamento para ocorrências

que possam evidenciar desvios nos processos relacionados à gestão de segurança da informação e privacidade.

6.1.2.5. Avaliação de riscos de segurança da informação e privacidade

Para avaliação de riscos de segurança da informação e privacidade, a organização mantém planos cujo objetivo é proteger os funcionários, contratados, fornecedores e clientes, na eventualidade de uma ocorrência ou crise. Segue:

- **Declaração de Aplicabilidade –** São avaliados controles pertinentes para a mitigação de riscos relacionados à segurança da informação e privacidade e as medidas tomadas em cada situação.
- **Análise de Riscos –** Análise e avaliação de riscos pertinentes para o sistema de gestão de segurança da informação e privacidade.

Além da Declaração de Aplicabilidade, o SGPI conta também com o PROC-SGSI-007 - Controle Operacional e Gestão de Riscos.

6.1.3. Checar

6.1.3.1. Monitoramento e medição

A **PSM Company** define através dos procedimentos PROC-SGSI-002 - Objetivos, Metas e Indicadores, PROC-SGSI-004 - Auditorias Internas, PROC-SGSI-007 - Controle Operacional e Gestão de Riscos e PROC-SGSI-008 - Análise Crítica pela Direção a sistemática para monitorar e medir os principais elementos do SGPI, incluindo objetivos e operações que sejam críticas ou significativas. São exemplos de monitoramento:

- controle de documentos legais;
- auditorias internas;
- acompanhamento do desempenho dos indicadores do SGPI.

6.1.3.2. Não Conformidade, ação corretiva e ação de melhoria

A **PSM Company** mantém o procedimento PROC-SGSI-005 - Gestão de Não Conformidades e Ações de Melhoria para registro, investigação e análise para tratamento de não conformidades reais e potenciais. Estes mesmos esforços podem tanto identificar a necessidade de ações corretivas, como oportunidades de ações de melhoria contínua.

6.1.3.3. Auditorias internas

Estão previstas auditorias internas focando a verificação de eficácia do SGPI e cumprimento dos requisitos e procedimentos relacionados a este Manual, conforme PROC-SGSI-004 - Auditorias Internas.

Os resultados são documentados e constituem pauta para Reuniões de Análise Crítica. Independentemente deste processo, as eventuais **NC**s o **OM**s (oportunidades de melhoria) devem ser tratadas tão logo sejam identificadas, conforme PROC-SGSI-005 - Gestão de Não Conformidades e Ações de Melhoria.

6.1.4. Agir

6.1.4.1. Análise Crítica

A Direção deve analisar o SGPI conforme PROC-SGSI-008 - Análise Crítica pela Direção, para assegurar sua contínua adequação, suficiência e eficácia. Essa análise deve incluir a avaliação de oportunidades para melhoria e necessidade de mudanças no SGPI, em todos os seus elementos.

7. ANEXO A – Controles e objetivos de controle - Controladores

7.1. Controles e objetivos de controle

Este anexo é usado pela **PSM Company** que atua como controladora de DP, com ou sem o uso de operadores de DP. Este anexo é uma extensão da ABNT NBR ISO/IEC 27001:2022, Anexo A.

Os controles e objetivos de controles acrescentados ou modificados listados na Tabela A.1 são diretamente derivados e estão alinhados com aqueles definidos neste documento e são para serem usados no contexto da ABNT NBR ISO/IEC 27001:2013, 6.1.3, como detalhado por 5.4.1.3. Nem todos os controles e objetivos de controles listados nesta Anexo precisam ser incluídos na implementação de um SGPI.

Uma justificativa para exclusão de quaisquer objetivos de controle deve ser incluída na Declaração de Aplicabilidade (ver 5.4.1.3). A justificativa para exclusão pode incluir situações em que os controles não são considerados necessários pela avaliação de riscos, e onde eles não sejam requeridos pela (ou estão sujeitos a exceções sob) regulamentação e/ou legislação aplicável.

NOTA: Os números das Seções neste Anexo estão relacionados com os números das subseções contidas na Seção 7 e 8 da ABNT NBR ISO/IEC 27001:2019.

7.2. Condições para coleta e tratamento

Seção	Requerimentos ISO/IEC 27701	Controles para Controladores ou Operadores	LGPD Correspondência	Controle	Documento
7.2.1	Identificação e documentação do propósito	**Controladores**	Art. 9º - I, Art. 14º § 6º Art.	A organização deve identificar e documentar os propósitos específicos pelos quais os DP serão tratados.	• PROC001-RS-Procedimento R&S • PROC001 ADM PESSOAL
7.2.2	Identificação de bases legais	**Controladores**	Art. 7º - II, Art. 8º § 4º, Art. 11º - IIa, Art.23º, Art. 26º - IV, Art. 34º - I	A organização deve determinar, documentar e estar em *compliance* com a base legal pertinente para o tratamento de DP para os propósitos identificados.	• TER039- DP referenciado no PROC001 ADM PESSOAL item 6
7.2.3	Determinando quando e como o consentimento deve ser obtido	**Controladores**	Art. 5º XII, Art. 7º, Art. 8º, Art. 11º, Art. 14.	A organização deve determinar e documentar um processo pelo qual ela possa demonstrar se, quando e como o consentimento para o tratamento de DP foi obtido dos titulares de DP.	• TER039- DP • TER025-DP Confidencialidade e da Segurança da Informação psmrecrutamento.com.br
7.2.4	Obtendo e registrando o consentimento	**Controladores**	Art. 5º XII, Art. 7º, Art. 8º, Art. 11º, Art. 14.	A organização deve obter e registrar o consentimento dos titulares de DP de acordo com os processos documentados.	• PROC001-RS-Procedimento R&S • PROC001 ADM PESSOAL, ITEM 3.1
7.2.5	Avaliação de impacto de privacidade	**Controladores**	Art. 4º - § 3º, Art. 5º XVII, Art. 10º III, Art. 32º, Art. 38º	A organização deve avaliar a necessidade para, e implementar onde apropriado, uma avaliação de impacto de privacidade quando novos tratamentos de DP ou	• PROC-SGSI-007-Controle Operacional e Gestão de Riscos

				mudanças ao tratamento existente de DP forem planejados.	
7.2.6	Contratos com operadores de DP	**Controladores**	Art. 7º, Art. 39º	A organização deve ter um contrato por escrito com qualquer operador de DP que ela utilize, e deve assegurar que os seus contratos com os operadores de DP contemplem a implementação de controles apropriados, conforme descrito no Anexo B	• Contrato com Operadores
7.2.7	Controlador conjunto de DP	**Controladores**	Art. 7º - § 5º	A organização deve determinar as responsabilidades e respectivos papéis para o tratamento de DP (incluindo a proteção de DP e os requisitos de segurança) com qualquer controlador conjunto de DP.	• SGSI_Organograma x Matriz RACI - Descrição de Cargos
7.2.8	Registros relativos ao tratamento de DP	**Controladores**	Art. 37º	A organização deve determinar e manter de forma segura os registros necessários ao suporte às suas obrigações para tratamento do DP	• POL001-TI Desenvolvimento Seguro • POL002-TI Tecnologia da Informacao • NOR006-TI Serviços de Cloud • PROC002-TI Backup e restore banco de dados • PROC005-TI Backup Restore Sharepoint Exchange • PROC014-TI Controle Acesso Lógico • PROC-011-DIR-Acesso Fisico a PSM

7.3. Obrigações dos titulares de DP

Seção	Requerimentos ISO/IEC 27701	Controles para Controladores ou Operadores	LGPD Correspondência	Controle	Documento
7.3.1	Determinando e cumprindo as obrigações para os titulares de DP	**Controladores**	Art. 9º	A organização deve determinar e documentar suas obrigações regulatórias, legais e de negócios para os titulares de DP, relativas ao tratamento de seus DP e fornecer meios para atender a estas obrigações.	• REG-SGSI-003 - REQUISITOS LEGAIS E OUTROS REQUISITOS_R00 • PROC-SGSI-003 - Requisitos Legais e Outros Requisitos
7.3.2	Determinando as informações para os titulares de DP	**Controladores**	Art. 9º	A organização deve determinar e documentar a informação a ser fornecida aos titulares de DP, relativa ao tratamento de seus DP, e o tempo de tal disponibilização.	• PROC021-TI Anonimização e Exclusão de Dados - LGPD
7.3.3	Fornecendo informações aos titulares de DP	**Controladores**	Art. 9º	A organização deve fornecer aos titulares de DP, de forma clara e facilmente acessível, informações que identifiquem o controlador de DP e descrevam o tratamento de seus DP	• PROC021-TI Anonimização e Exclusão de Dados - LGPD
7.3.4	Fornecendo mecanismos para modificar ou cancelar o consentimento	**Controladores**	Art. 8º § 5º, Art. 9º § 2º	A organização deve fornecer mecanismos para os titulares de DP para modificar ou cancelar os seus consentimentos.	• PROC021-TI Anonimização e Exclusão de Dados - LGPD
7.3.5	Fornecendo mecanismos para negar o consentimento ao tratamento de DP	**Controladores**	Art. 8º § 5º, Art. 9º § 2º	A organização deve fornecer mecanismos para os Î titulares de DP para negar o consentimento ao tratamento do seus DP	• PROC001-RS-Procedimento R&S

7.3.6	Acesso, correção e/ou exclusão	**Controladores**	Art. 9º	A organização deve implementar políticas, procedimentos e/ou mecanismos para atender às suas obrigações para os titulares de DP acessarem, corrigirem e/ou excluírem os seus DP	• PROC009ADMP - ATUALIZAÇÃO CADASTRAL
7.3.7	Obrigações dos controladores de DP para informar aos terceiros	**Controladores**	Art. 18º § 6º	A organização deve informar aos terceiros com quem o DP foi compartilhado sobre qualquer modificação, cancelamento ou desaprovação pertinente ao DP compartilhado, e implementar políticas e procedimentos apropriados e/ou mecanismos para fazê-lo	• PROC008-ADMP - Processo de demissão • PROC009-ADMP Atualização Cadastral
7.3.8	Fornecendo cópia do DP tratado	**Controladores**	Art. 18º II	A organização deve ser capaz de fornecer uma cópia do DP que é tratado, quando requerido pelo titular de DP.	• PROC021- Anonimização e Exclusão de Dados - LGPD • PROC020-SI - Direito a confirmação da existência do tratamento • FOR020-SI - Direito dos Titulares de DP • POL020-SI Política de Gestão de Dados
7.3.9	Tratamento de solicitações	**Controladores**	Art. 18º	A organização deve definir e documentar políticas e procedimentos para tratamento e respostas, a solicitações legítimas dos titulares de DP	• PROC021- Anonimização e Exclusão de Dados - LGPD • PROC020-SI - Direito a confirmação da existência do tratamento • FOR020-SI - Direito dos Titulares de DP • POL020-SI Política de Gestão de Dados
7.3.10	Tomada de decisão automatizada	**Controladores**	Art. 18º	A organização deve identificar e considerar as obrigações, incluindo obrigações legais, para os titulares de DP, como resultado das decisões feitas pela organização que estejam relacionadas ao	• PROC001 ADMPESSOAL - ADMISSÃO E INTEGRAÇÃO, PROC008 ADMP - PROCESSOS DE DEMISSÃO • POL020-SI Política de Gestão de Dados

				titular de DP, baseadas unicamente no tratamento de DP.	

7.4. Privacy by Design e Privacy by Default

Seção	Requerimentos ISO/IEC 27701	Controles para Controladores ou Operadores	LGPD Correspondência	Controle	Documento
7.4.1	Limite de coleta	**Controladores**	Art. 6º - III	A organização deve limitar a coleta de DP a um mínimo que seja relevante, proporcional e necessário para os propósitos identificados.	• PROC003 ADMP-PCMSO E ATESTADOS • PROC007 ADMP Benefícios
7.4.2	Limite de tratamento	**Controladores**	Art. 16º	A organização deve limitar o tratamento de DP de tal forma que seja adequado, relevante e necessário para os propósitos identificados.	• PROC003 ADMP-PCMSO E ATESTADOS • PROC007 ADMP Benefícios
7.4.3	Precisão e qualidade	**Controladores**	Art. 6º - V	A organização deve assegurar e documentar que o DP é preciso, completo e atualizado, como é necessário para os propósitos aos quais ele é tratado, por meio do ciclo de vida do DP	• Planilha - Gestão de Operação de Dados Pessoais
7.4.4	Objetivos de minimização de DP	**Controladores**	Art. 6º - II CAPÍTULO VII	A organização deve definir e documentar os objetivos da minimização dos dados e quais mecanismos (como a anonimização) são usados para atender àqueles objetivos.	• PROC001 ADMPESSOAL - ADMISSÃO E INTEGRAÇÃO, • PROC001-RS - PROCEDIMENTO • POL001 - TI - Desenvolvimento seguro/(MD5)

7.4.5	Anonimização e exclusão de DP ao final do tratamento	**Controladores**	Art. 16º	A organização deve excluir DP ou entregá-lo na forma que não permita a identificação ou reidentificação dos titulares de DP, uma vez que o DP original não é mais necessário para os propósitos identificados	• PROC001 ADMPESSOAL - ADMISSÃO E INTEGRAÇÃO, • PROC001-RS - PROCEDIMENTO • POL001 - TI - Desenvolvimento seguro/(MD5)
7.4.6	Arquivos temporários	**Controladores**	CAPÍTULO VII	A organização deve assegurar que os arquivos temporários criados como um resultado de tratamento de DP sejam descartados (por exemplo, apagados ou destruídos) seguindo procedimentos documentados dentro de um período documentado, especificado.	• PROC0010- ADMPESSOAL -DESCARTE DE DADOS
7.4.7	Retenção	**Controladores**	Art. 16º	A organização não pode reter o DP por um tempo maior do que é necessário para os propósitos para os quais o DP é tratado.	• PROC0010- ADMPESSOAL -DESCARTE DE DADOS
7.4.8	Descarte	**Controladores**	CAPÍTULO VII	A organização deve ter políticas, procedimentos e/ou mecanismos documentados para o descarte de DP	• PROC0010- ADMPESSOAL -DESCARTE DE DADOS
7.4.9	Controle de transmissão de DP	**Controladores**	CAPÍTULO VII	A organização deve tratar DP transmitido (por exemplo, enviado para outra organização) que trafegue por uma rede de transmissão de dados, com controles apropriados concebidos para assegurar que os dados alcancem seus destinos pretendidos.	• PROC013-TI Transferência de Arquivos; • PROC014-TI Controle Acesso Lógico; • NOR005-SI Classificação da Informação PSM; • PROC004;005/006/007/008

7.5. Compartilhamento, transferência e divulgação de DP

Seção	Requerimentos ISO/IEC 27701	Controles para Controladores ou Operadores	LGPD Correspondência	Controle	Documento
7.5.1	Identificando as bases para a transferência de DP entre jurisdições	**Controladores**	Art. 7º	A organização deve identificar e documentar as bases relevantes para a transferência de DP entre jurisdições	• PROC001 - FATU - PROCESSO DE FATURAMENTO PSM v2.0.0 - envio de racionais e valores para cobrança • PROC001 – PV PSM v2.0.0 – Gestão de Clientes • 00.PROC003 - NN - Elaboração de proposta comercial V0 • PROC013-TI Transferência de Arquivos e planilha de gestão de Operações de dados pessoais; • PROC001-ADMP-ADMISSÃO; • PROC003ADMP-PCMSO E ATESTADOS; • PROC007-ADMP-BENEFICIOS
7.5.2	Países e organizações internacionais para os quais os DP podem ser transferidos.	**Controladores**	CAPÍTULO V	A organização deve especificar e documentar os países e as organizações internacionais para os quais o DP possam possivelmente ser transferidos.	
7.5.3	Registros de transferência de DP	**Controladores**	CAPÍTULO V	A organização deve registrar a transferência de DP para ou de terceiros e assegurar a cooperação com essas partes para apoiar futuras solicitações relativas às obrigações para os titulares de DP.	• PROC013-TI Transferência de Arquivos • PROC014-TI Controle Acesso Lógico • NOR005-SI Classificação da Informação PSM
7.5.4	Registro de divulgação de DP para terceiros	**Controladores**	Art. 37º	A organização deve registrar a divulgação de DP para terceiros, incluindo qual DP foi divulgado, para quem e quando	• PROC007-ADMP BENEFÍCIOS • PROC013-TI Transferência de Arquivos • NOR005-SI Classificação da Informação PSM • PROC014-TI Controle Acesso Lógico

8. ANEXO B - Controles e objetivos de controle- - Operadores

8.1. Controles e objetivos de controle

Este Anexo deve ser usado pelas organizações que atuam como operadores de DP, com ou sem o uso de subcontratados de DP. Ele é uma extensão da ABNT NBR ISO/IEC 27001:2013, Anexo A.

Os controles e objetivos de controles modificados ou acrescentados listados na Tabela B.1 são diretamente derivados e estão alinhados com aqueles definidos neste documento e são para serem usados no contexto da ABNT NBR ISO/IEC 27001:2013, 6.1.3, como detalhado por 5.4.1.3. Nem todos os controles e objetivos de controles listados nesta Anexo precisam ser incluídos na implementação de um SGPI.

Uma justificativa para exclusão de quaisquer objetivos de controle deve ser incluída na Declaração de Aplicabilidade (ver 5.4.1.3). A justificativa para exclusão pode incluir situações em que os controles não sejam considerados necessários pela avaliação de riscos, e onde eles não sejam requeridos pela (ou estejam sujeitos a exceções sob) regulamentação e/ou legislação aplicável.

NOTA Os números das seções neste Anexo estão relacionados com os números das subseções contidas na Seção 8.

8.2. Condições para coleta e tratamento

Seção	Requerimentos ISO/IEC 27701	Controles para Controladores ou Operadores	LGPD Correspondência	Controle	Documento
8.2.1	Acordos com o cliente	**Operadores**	Artigo 10o, I, II Artigo 18º.	A organização deve assegurar, onde pertinente, que o contrato para tratar DP considera os papéis da organização em fornecer assistência com as obrigações	• PROC002 - FATU - CONTROLE DE CONTRATOS DE CLIENTES - Contratos com os clientes / procedimentos de transferência de arquivos + (A.7.5.1) + Aditivo de Contrato de Operadores;

				do cliente (considerando a natureza do tratamento e a informação disponível para a organização).	• PROC001-ADMP-ADMISSÃO; • PROC003ADMP-PCMSO E ATESTADOS; • PROC007-ADMP-BENEFICIOS
8.2.2	Propósitos da organização	**Operadores**	Artigo 9o, I, II, III, IV, V, VI, VII Artigo 23º.	A organização deve assegurar que os DP tratados em nome do cliente sejam apenas tratados para o propósito expresso nas instruções documentadas do cliente.	• PROC002 - FATU - CONTROLE DE CONTRATOS DE CLIENTES - Contratos com os clientes / procedimentos de transferência de arquivos + (A.7.5.1) Aditivo de Contrato de Operadores; • PROC001-ADMP-ADMISSÃO; • PROC003ADMP-PCMSO E ATESTADOS; • PROC007-ADMP-BENEFICIOS
8.2.3	Uso de marketing e propaganda	**Operadores**	Artigo 6º. Artigo 9o, I, II, III, IV, V, VI, VII Artigo 10º., I	A organização não pode utilizar os DP tratados sob um contrato para marketing e propaganda, sem o estabelecimento de que um consentimento antecipado foi obtido do titular de DP apropriado. A organização não pode fornecer este consentimento como uma condição para oÎ recebimento do serviço.	• Contratos firmados com os clientes
8.2.4	Violando instruções	**Operadores**	Artigo 44º. Artigo 45º.	A organização deve informar ao cliente se, na sua opinião, uma instrução de tratamento viola uma regulamentação e/ou legislação aplicável.	• PROC-SGSI-003 - Requisitos Legais e Outros Requisitos
8.2.5	Obrigações do cliente	**Operadores**	Artigo 44º	A organização deve fornecer ao cliente informações apropriadas de tal modo que o cliente possa demonstrar compliance com suas obrigações.	• PROC002 - FATU - CONTROLE DE CONTRATOS DE CLIENTES - Contratos com clientes / Procedimentos. • PROC013-TI Transferência de Arquivos; Zenilda: não tem procedimento documentado, mas a rotina é executada como descrito.

8.2.6	Registros relativos ao tratamento de DP	**Operadores**	Artigo 37º	A organização deve determinar e manter os registros necessários para apoiar a demonstração do *compliance* com suas obrigações (como especificado no contrato aplicável) para tratamento de DP realizado em nome do cliente.	• PROC001ADMP-ADMISSÃO E INTEGRAÇÃO; • PROC004ADMP- FOLHA DE PAGAMENTO E ESOCIAL • PROC008 -DEMISSÃO PROC007-ADMP BENEFÍCIOS / Prodecimento de Transferencias de Arqivos + Procedimento de contrataçao/Integração e de R&S/ Acordo de confidencialidade entre outros... • PROC001-RS-Procedimento R&S

8.3. Obrigações dos titulares de DP

Seção	Requerimentos ISO/IEC 27701	Controles para Controladores ou Operadores	LGPD Correspondência	Controle	Documento
8.3.1	Obrigações para os titulares de DP	**Operadores**	Artigo 6º., I, II, III, IV, V, VI, VII, VIII, IX, X Artigo 7º., I, II, III, IV, V, VI, VII, VIII, IX, X Artigo 42º.	A organização deve fornecer ao cliente meios para estar em *compliance* com suas obrigações relativas aos titulares de DP	• PROC001-RS-Procedimento R&S • PROC001 ADM PESSOAL - ADMISSÃO E INTEGRAÇÃO; • TERMO DE CONSENTIMENTO PARA TRATAMENTO DE DADOS (Antes do preenchimento de DP e anexar os documentos no Conecta)

8.4. Privacy by design e privacy by default Obrigações

Seção	Requerimentos ISO/IEC 27701	Controles para Controladores ou Operadores	LGPD Correspondência	Controle	Documento

8.4.1	Arquivos temporários	**Operadores**	Artigo 46º. Artigo 49º.	A organização deve assegurar que os arquivos temporários criados como um resultado do tratamento de DP sejam descartados (por exemplo, apagados ou destruídos) seguindo os procedimentos documentados, dentro de um período especificado e documentado.	• PROC0010- ADMPESSOAL -DESCARTE DE DADOS
8.4.2	Retorno, transferência ou descarte de DP	**Operadores**	Artigo 15º., I, II, III, IV Artigo 16º., I, II, III, IV Artigo 46º.	A organização deve fornecer a capacidade de retornar, transferir e/ou descartar DP de uma maneira segura. Deve também tornar sua política disponível para o cliente.	• PROC021-TI Anonimização e Exclusão de Dados - LGPD • PROC013-TI Transferência de Arquivos • PROC006-TI PSM-Procedimento de Descarte Seguro
8.4.3	Controles de transmissão de DP	**Operadores**	Artigo 6º., VII, VIII Artigo 37º. Artigo 46º.	A organização deve sujeitar DP transmitidos sobre uma rede de transmissão de dados a controles apropriados projetados, para assegurar que os dados alcancem seus destinos pretendidos.	• PROC013-TI Transferência de Arquivos • NOR005-SI Classificação da Informação PSM • PROC003-TI Criptografia de discos - Bitlocker • NOR009 - TI CRIPTOGRAFIA EM DISPOSITIVOS MOVEIS

8.5. Compartilhamento, transferência e divulgação de DP

Seção	Requerimentos ISO/IEC 27701	Controles para Controladores ou Operadores	LGPD Correspondência	Controle	Documento
8.5.1	Bases para a transferência de DP entre jurisdições	**Operadores**	Artigo 33º., I, II, III, IV, V, VI, VII, VIII, IX	A organização deve informar ao cliente em um tempo hábil sobre as bases para a transferência de DP entre jurisdições e de qualquer mudança pretendida nesta	• PROC001 - FATU - PROCESSO DE FATURAMENTO PSM v2.0.0 - envio de racionais e valores para cobrança • PROC001 – PV PSM v2.0.0 – Gestão de Clientes • 00.PROC003 - NN - Elaboração de proposta comercial V0

			Artigo 34º., I, II, III, IV, V, VI	questão, de modo que o cliente tenha a capacidade de contestar estas mudanças ou rescindir o contrato.	• PROC013-TI Transferência de Arquivos • PROC-SGSI-003 - Requisitos Legais e Outros Requisitos
8.5.2	Países e organizações internacionais para os quais DP podem ser transferidos	**Operadores**	Artigo 33º., I, II, III, IV, V, VI, VII, VIII, IX Artigo 34º., I, II, III, IV, V, VI	A organização deve especificar e documentar os países e as organizações internacionais para os quais DP possam, possivelmente, ser transferidos.	• Conforme documento P0L020-SI Política de Gestão de Dados item 15
8.5.3	Registros de DP divulgados para terceiros	**Operadores**	Artigo 16º. Artigo 37º.	A organização deve registrar a divulgação de DP para terceiros, incluindo quais DP foram divulgados, para quem e quando	• PROC007-ADMP BENEFÍCIOS • PROC013-TI Transferência de Arquivos • NOR005-SI Classificacao da Informacao PSM • PROC014-TI Controle Acesso Lógico
8.5.4	Notificação de solicitações de divulgação de DP	**Operadores**	Artigo 6º., I, VI Artigo 41º.	A organização deve notificar ao cliente sobre quaisquer solicitações legalmente obrigatórias para a divulgação de DP.	• POL020 -SI Política de Gestão de Dados
8.5.5	Divulgações legalmente obrigatórias de DP	**Operadores**	Artigo 4º., III, IV Artigo 41º.	A organização deve rejeitar quaisquer solicitações para a divulgação de DP que não sejam legalmente obrigatórias, consultar o cliente em questão antes de realizar quaisquer divulgações do DP e aceitar quaisquer solicitações contratualmente acordadas para a divulgação de DP, que sejam autorizadas pelo respectivo cliente.	• POL020 -SI Política de Gestão de Dados
8.5.6	Divulgação de subcontratados usados para tratar DP	**Operadores**	Artigo 41º.	A organização deve divulgar para o cliente qualquer uso de subcontratados para tratar DP, antes do uso	

8.5.7	Contratação de um subcontratado para tratar DP	**Operadores**	. Artigo 39º. Artigo 41º.	A organização deve somente contratar um subcontratado para tratar DP com base no contrato do cliente.	
8.5.8	Mudança de subcontratado para tratar DP	**Operadores**	Artigo 39º. Artigo 41º.	A organização deve, no caso de ter uma autorização geral por escrito, informar o cliente de quaisquer alterações pretendidas relativas à adição ou substituição de subcontratados no tratamento de DP, dando assim ao cliente a oportunidade de se opor a essas alterações.	

<FIM DO DOCUMENTO>