CRCPR
CONSELHO REGIONAL DE CONTABILIDADE DO PARANÁ

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Implantação da Lei Geral de
Proteção de Dados Pessoais (LGPD)
Lei n.º 13.709, 14 de agosto de 2018

Curitiba (PR)

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Implantação da Lei Geral de Proteção de Dados Pessoais (LGPD)

CONSELHO REGIONAL DE CONTABILIDADE DO PARANÁ
Rua XV de Novembro, 2987 - Alto da XV
CEP: 80045-340 – Curitiba (PR) – Brasil
Fone: 55 (41) 3360-4700
E-mail: crcpr@crcpr.org.br
Site: www.crcpr.org.br

Presidente
Everson Luiz Breda Carlin

Diretor Superintendente
Gerson Luiz Borges de Macedo

Coordenadora de Governança
Nadja Nayra Baptista Andreacci

Equipe Técnica
Comissão de Governança, Riscos, Compliance e LGPD do CRCPR

Produção Gráfica/Editorial
Divisão de Comunicação

Revisão
Adriana Iaizzo Magalhães

Projeto Gráfico e Diagramação
Flavia Norberto

Curitiba, agosto de 2025.

SUMÁRIO

03
Justificativa
Objetivo Geral
Objetivos Específicos
Meta
Fonte

04
Etapa 1
Iniciação e Planejamento
Entregáveis da Etapa 1
Etapa 2
Construção e Execução
Entregáveis da Etapa 2

05
Etapa 3
Monitoramento
Entregáveis da Etapa 3
Plano de Ação
Plano de Trabalho

06
Desafios Enfrentados
Envolvimento do Corpo Funcional
Mensuração dos Resultados
Conclusão

07
Etapa 1
Iniciação e Planejamento

08
Etapa 2
Construção e Execução

11
Etapa 3
Monitoramento

PROGRAMA DE GOVERNANÇA EM PRIVACIDADE

Implantação da Lei Geral de Proteção de Dados Pessoais (LGPD)

JUSTIFICATIVA

A Lei n.º 13.709, de 14 de agosto de 2018, que trata da Lei Geral de Proteção de Dados Pessoais (LGPD), dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

As normas gerais contidas na LGPD são de interesse nacional e devem ser observados pela União, estados, Distrito Federal e municípios. Por esse motivo, e considerando a normatização dessa temática no cenário mundial, o presente programa visa à adequação do Conselho Regional de Contabilidade do Paraná (CRCPR) à Lei Geral de Proteção de Dados.

O CRCPR tem compromisso com a segurança das informações e a responsabilidade em adotar o conjunto de regras e boas práticas de governança para promover a cultura da privacidade e da proteção de dados pessoais dos titulares da informação no âmbito dos Conselhos de Contabilidade, por meio de publicações, e da realização de seminários, palestras, cursos, campanhas, entre outras ações para tratar desse tema.

OBJETIVO GERAL

Definir as diretrizes e regras gerais para o tratamento de dados pessoais no âmbito do CRCPR, com o objetivo de proteger a privacidade dos profissionais da contabilidade, das organizações contábeis, empregados, parceiros, fornecedores e sociedade tendo como foco a gestão de dados pessoais e a gestão de incidentes de Segurança da Informação no ambiente convencional ou de tecnologia, em conformidade com a LGPD.

OBJETIVOS ESPECÍFICOS

a) Orientar as suas unidades organizacionais quanto à adequação e aplicação da LGPD;

b) Garantir que a privacidade e a proteção de dados pessoais seja parte do cotidiano das atividades e funções desempenhadas pelo CRCPR de forma a proteger o titular da informação quanto ao processamento, tratamento e livre circulação de seus dados pessoais;

c) Contratar empresa especializada na prestação de serviços de consultoria para auxiliar a efetiva implantação da LGPD;

d) Adquirir software especializado para gerenciar e conduzir a aplicação da LGPD;

e) Elaborar políticas e planos de proteção de dados pessoais e privacidade do CRCPR

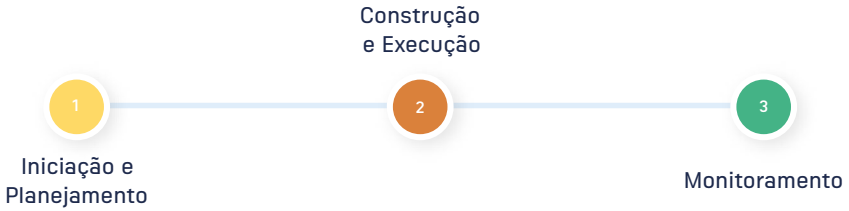
META

Estruturar o CRCPR para assegurar a adequada conformidade à LGPD até 31 de dezembro de 2022.

FONTE

Guias do Governo Federal: Mais informações acesse

ETAPAS



ETAPA 1 – Iniciação e Planejamento

Compreensão de quais são as primeiras informações e dados importantes que devem ser conhecidos.

1	Nomeação do encarregado de dados (DPO)
2	Alinhamento de expectativas com a alta administração
3	Análise da maturidade – diagnóstico do atual estágio de adequação à LGPD
4	Análise e adoção de medidas de segurança, inclusive diretrizes e cultura interna
5	Instituição de estrutura organizacional para governança e gestão da proteção de dados pessoais
6	Inventário de dados pessoais
7	Levantamento dos contratos relacionados a dados pessoais

Entregáveis da Etapa 1:

N.º	Item	Entrega
1	Portaria que designa o DPO	22/12/2020
2	Portaria que constitui a Comissão de Implantação da LGPD	18/03/2021
3	Portaria que cria Comitê de Segurança da Informação	18/03/2021
4	Incluir aba LGPD no site do CRCPR	19/01/2021
5	Canal de interação com o DPO	19/01/2021
6	Reunião de *Kickoff*	13/04/2021
7	Workshop de conscientização com os empregados	23/04/2021
8	Solicitação de documentos	20/04/2021
9	Retorno dos documentos	27/04/2021
10	Envio de formulário de TI	19/04/2021
11	Resposta do formulário de TI	27/04/2021
12	Visita presencial	22/04/2021
13	Questionário online para os empregados	15/6/2020
14	Entrevistas individuais com gestores	24 a 26/05/2021
15	Análise de maturidade - diagnóstico da situação atual	21/06/2021
16	Plano de Ação	21/06/2021
17	Inventário de dados pessoais	21/06/2021
18	Levantamento de contratos relacionados a dados pessoais	21/06/2021
19	Reuniões com a Consultoria	Mensal
20	Reuniões com a Comissão	Mensal

ETAPA 2 – Construção e Execução

Construção e execução de marcos que protegem os direitos do cidadão em relação à privacidade da informação.

1	Políticas e práticas para proteção da privacidade
2	Cultura de segurança e proteção de dados e Privacy by Design
3	Relatório de Impacto sobre a Proteção de Dados Pessoais (RIPD)
4	Política de Privacidade e Política de Segurança da Informação
5	Adequação de cláusulas contratuais
6	Termo de Uso

Entregáveis da Etapa 2:

N.º	Item	Entrega
1	Resposta à requisição da ANPD	28/07/2021
2	Anonimização, bloqueio e exclusão de dados	21/10/2021
3	Plano de Continuidade de Negócios	29/10/2021
4	Política de BYOD*	Sobrestado
5	Política de Acesso Remoto	29/10/2021
6	Política de Segurança Cibernética	29/10/2021

*Bring Your Own Device -acesso a sistemas da instituição com equipamentos pessoais (ex.: smartphone)

7	Manual de Backup	29/10/2021
8	Política de Privacidade	29/10/2021
9	Política de Cookies	24/09/2021
10	Política de Segurança da Informação	11/04/2022
11	Classificação da Informação	11/04/2022
12	Aditivo contratual - parceiros	27/05/2022
13	Termo aditivo - contabilista	Em andamento
14	Termo aditivo - empregados	26/05/2022
15	Termo de Cessão Uso de Imagem	26/05/2022
16	Termo de Sigilo de Delegados	28/01/2022
17	Revogação do Consentimento	26/05/2022
18	Política de Registro de Incidentes	11/04/2022
19	Termo de Rescisão	26/05/2022
20	Política de Gestão de Riscos	26/05/2022
21	Política de Relacionamento com terceiros	26/05/2022
22	Política de Sustentabilidade	26/05/2022
23	Orientações para realização de eventos	26/05/2022
24	Relatório de Impacto RIPD	02/12/2022
25	Plano de Comunicação Interna	02/12/2022
26	Plano de treinamento e desenvolvimento PD	02/12/2022
27	Gestão de Riscos relacionados à LGPD	02/12/2022
28	Termo de Conselheiros	03/03/2022
29	Política de Eventos	26/05/2022
30	Treinamento com Alta Direção e empregados	02/12/2022

ETAPA 3 – MONITORAMENTO

Acompanhamento da conformidade à LGPD.

1	Indicadores de performance
2	Gestão de Incidentes
3	Análise de resultados
4	Reporte de resultados

Entregáveis da Etapa 3:

N.º	Item	Entrega
1	Relatório com os resultados alcançados	Mensal
2	Relatório de auditoria	ago/24
3	Registro de incidentes de segurança da informação	Não houve
4	Relatório de análise de riscos	22/11/2023
5	Resultado dos indicadores de desempenho	05/12/2023

Plano de Trabalho

Objetivo estratégico: 5 – Atuar como fator de proteção da sociedade.
Programa: Suporte e apoio a atividades fins.
Projeto: 5028 – Governança da Informação.
Responsável: Vice-Presidência de Administração e Finanças

Plano de ação

Detalhamento das ações de cada etapa.
Páginas a seguir.
Atualização diária.

Desafios enfrentados

Os principais desafios foram o entendimento da legislação específica, a verificação da forma de colocar em prática as diretrizes da LGPD, a adaptação dos sistemas informatizados para atendimento da lei, a sensibilização do corpo funcional do CRCPR, a identificação do fluxo dos dados pessoais nos projetos executados pelas Unidades Organizacionais do CRCPR e a elaboração de normativos com a finalidade de adequação à Lei n.º 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD).

Envolvimento do corpo funcional

Diante da importância do corpo funcional nesse trâmite, os empregados foram inseridos no processo desde o início, por meio de treinamentos, workshops, bate-papos, campanhas de comunicação interna e entrevistas individuais para o levantamento e a identificação dos dados pessoais tratados em cada área, com o objetivo de construir um inventário completo dos dados pessoais armazenados nas bases do CRCPR.

Mensuração dos resultados

A Comissão de Governança, Riscos, Compliance e LGPD do CRCPR, através dos indicadores de desempenho monitora os resultados do Programa de Governança em Privacidade. Foram utilizadas as sugestões de indicadores do guia do governo federal, com alterações de acordo com a realidade do CRCPR, e foram estabelecidos 5 indicadores com apuração semestral. A planilha de controle contém os campos: indicador, objetivo, fórmula do indicador, meta, fonte, frequência de apuração, registros e responsável. Os primeiros resultados foram registrados em julho de 2022.

Conclusão

Com a conclusão dos documentos, o CRCPR finalizou as diretrizes e regras gerais para o tratamento de dados pessoais no âmbito da entidade, protegendo a privacidade de profissionais da contabilidade, organizações contábeis, empregados, parceiros, fornecedores e sociedade, tendo como foco a gestão de dados pessoais e a gestão de incidentes de segurança da informação no ambiente convencional ou de tecnologia, em conformidade com a LGPD. Além disso, o atendimento à LGPD trouxe um ambiente mais seguro ao CRCPR para tratar os dados pessoais. Dessa forma, o CRCPR conta com um corpo funcional mais capacitado e consciente, e com um parque tecnológico mais atualizado e seguro.

Etapa 1 - Iniciação e Planejamento					
Nº	**Ação de melhoria**	**Motivo**	**Responsável**	**Atividades desenvolvidas**	**Status**
1	Definir Encarregado/DPO	A Diretoria definirá o perfil do profissional que atuará como Encarregado/DPO, baseado nos requisitos impostos pela LGPD. Ou ainda, definirá pela contratação de empresa que preste esse serviço.	Diretoria	1 - Escolher profissional que será responsável de acordo com critérios estabelecidos pela lei; 2 - Publicizar decisão para demais departamentos da empresa; 3 - Publicizar decisão para público externo por meio de forma de comunicação a ser escolhida (e-mail, site, notificação, etc.).	**Concluído**
2	Criação de canal de comunicação com o DPO	A LGPD exige que o DPO seja de fácil e rápido acesso. Dessa forma, é imperiosa a criação de um canal de comunicação de fácil acesso e gratuito, preferencialmente no site do cliente. Da mesma forma, sugere-se que o canal de ouvidoria tenha a possibilidade de anonimato - para os próprios empregados.	Diretoria	1 - Criar um canal de comunicação que melhor se adeque à empresa 2 - Disponibilizar nesse canal o nome do DPO 3 - As informações de contato do DPO deverão ser divulgadas publicamente, de forma clara e objetiva.	**Concluído**
3	Capacitar os integrantes da Comissão de Implantação da Lei Geral de Proteção de Dados (LGPD).	Conceitos legais importantes da LGPD, dicas de boas práticas de segurança da informação, necessidade de engajamento dos profissionais, etapas nas quais os profissionais deverão estar engajados e sugestões de documentários sobre privacidade e proteção de dados;	RH	Treinamento que engloba mapeamento de processos, questões jurídicas e legislativas, tecnologia da informação e segurança cibernética; - Orientação de boas práticas correlacionadas a cada setor da empresa – Orientação de cada setor da empresa, com questões de boas práticas de segurança da informação, para os processos desenvolvidos.	**Concluído**
4	Reunião inicial	Apresentação de metodologia, plano de comunicação, cronograma, e formato do status report, com solução de dúvidas e definições necessárias ao andamento do projeto;	Comissão	Explicação para os gestores e empregados de conceitos legais importantes da LGPD, dicas de boas práticas de segurança da informação, necessidade de engajamento dos profissionais, etapas nas quais os profissionais deverão estar engajados e sugestões de documentários sobre privacidade e proteção de dados.	**Concluído**
5	Mapear os processos internos nos quais ocorre o tratamento de dados pessoais ou dados pessoais sensíveis no âmbito do CFC	Questionário on-line para 100% dos profissionais que tratam dados, - Entrevistas individuais com gestores da empresa.	Comissão	Objetivo de identificar o fluxo das informações na organização, os processos desenvolvidos por cada área da empresa, com identificação dos dados pessoais aos quais o setor tem acesso, a forma de tratamento (físico/digital), o meio de recebimento e armazenamento, a finalidade para o uso, existência de tabela de temporalidade de exclusão.	**Concluído**
6	Relatório de impacto à proteção de dados	Elaborar RIPD para identificar e mitigar riscos à privacidade dos titulares de dados em processos que envolvem tratamento de dados pessoais, garantindo conformidade com a LGPD e segurança jurídica.	Comissão	Documentar a preocupação da organização com a proteção de dados pessoais, podendo ser utilizado, inclusive como prova dos esforços internos para avaliar e abordar riscos à privacidade e proteção de dados	**Concluído**
7	Matriz de risco	Elaborar a matriz de risco para identificar, avaliar e priorizar riscos, para minimizar impactos negativos em projetos, processos e operações.	Comissão	Tabela de severidade, baseada em probabilidade de ocorrência e impacto do evento danoso, se ocorrer incidente envolvendo dados pessoais, com graduação dos riscos para priorização de atividades na fase de implementação;	**Concluído**
8	Elaborar e ministrar periodicamente treinamento sobre a proteção de dados aos empregados do CRCPR	Analisando os pontos chave da LGPD relacionado a cultura organizacional, o RH deverá elaborar e ministrar treinamentos para os atuais empregados para disseminação de conhecimento e construção da nova cultura.	RH	1 - Fornecer aos empregados treinamento sobre como tratar os dados pessoais e sensíveis; 2- Quais cuidados são necessários na execução das atividades 3 - Vulnerabilidades e sugestão de melhorias	**Concluído**
9	Plano de ação para implementação completa da LGPD	Elaborar plano de ação para implementação da LGPD é organizar e direcionar as atividades necessárias para garantir a conformidade legal.	Comissão	Detalhamento de todas as atividades que devem ser realizadas na etapa de implementação, para que a empresa esteja em conformidade com a LGPD.	**Concluído**
10	Atualização de departamento de Compliance e/ou Gestão de Risco	Atualização de departamento responsável pela manutenção e atualização das políticas e procedimentos. Assim como, com a finalidade de garantir a continuidade dessas, por meio de controles internos especificos.	Comissão	1 - Elaborar as políticas da empresa 2 - Atualização constante das políticas 3 - Analisar os riscos de negócios da empresa 4 - Conhecer as leis, normas e regulamentos aplicáveis às atividades da empresa 5 - Desenvolver projetos de melhoria 6 - Disseminar o compliance 7 - Monitorar a segurança da informação	**Concluído**

Etapa 2 - Construção e Execução					
Nº	**Ação de melhoria**	**Motivo**	**Responsável**	**Atividades desenvolvidas**	**Status**
11	Criação de política de cookies	Criação de política que a ser publicada no site do CRCPR para demonstrar transparência no tratamento de dados para interessados externos.	DPO e Informática	Elaborar Política de cookies, criação de pop-up tratando sobre política de consentimento de cookies e política de privacidade, o que deve ser observado pelos controladores e operadores, em consonância com as boas práticas e de governança disciplinadas no art. 50 da Lei nº 13.709/2018	**Concluído**
12	Criação de política de privacidade	Criação de política que a ser publicada no site do CRCPR para demonstrar transparência no tratamento de dados para interessados externos.	DPO e Informática	1 - Elaborar a política de privacidade da empresa detalhando todas as informações, dados que são colhidos/utilizados e para qual finalidade 2 - O documento deve ser bem escrito e detalhado 3 - Deve explicar sobre a coleta de dados e registros das atividades, sobre a publicidade, sobre o armazenamento, os direitos dos titulares, as bases legais e o que mais a empresa julgar necessário	**Concluído**
13	Criação de política de segurança da informação	Revisão de política que vise à segurança das informações existentes na empresa, principalmente no que contende aos dados pessoais, com base na LGPD e ISO 27001.	Informática	1 - Revisar a política de segurança da informação, estabelecendo as diretrizes gerais para a gestão da informação da empresa. 2 - A política deve adotar critérios técnicos e administrativos aptos a proteger os dados pessoais de acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração ou qualquer forma de tratamento inadequado.	**Concluído**
14	Criação de política de autenticação de senhas	Formalização da política de criação e autenticação de senhas, revisando eventuais fragilidades no processo, com base na LGPD.	Informática	Recomenda-se a implantação da complexidade de senhas no AD e nos sistemas da empresa, além da troca periódica das senhas. De acordo com a ISO 27002: Sistema de gerenciamento de senha; Controle, Convém que sistemas para gerenciamento de senhas sejam interativos e assegurem senhas de qualidade com diretrizes que obrigue o uso individual de ID de usuário e senha para manter responsabilidades; permita que os usuários selecionem e modifiquem suas próprias senhas, incluindo um procedimento de confirmação para evitar erros; obrigue a escolha de senhas de qualidade; obrigue os usuários a mudarem as suas senhas temporárias no primeiro acesso ao sistema; force as mudanças de senha a intervalos regulares, conforme necessário; mantenha um registro das senhas anteriores utilizadas e bloquei a reutilização.	**Concluído**
15	Criação de política de utilização de e-mail	Formalização da política de utilização de conta de e-mail, analisando fragilidades e visando a atender à LGPD.	Informática	Estabelecer critérios sobre o uso, responsabilidade, forma, monitoramento, conteúdo do e-mail no ambiente corporativo.	**Concluído**
16	Criação de política de acesso à internet	Criar ou formalizar política existente de acessos à internet, com definição de blacklist e bloqueio de acessos, com intuito de atender à LGPD.	Informática	Estabelecer critérios sobre a utilização da internet no ambiente corporativo, abordar sobre a utilização para o desempenho de atividades profissionais do usuário, vedação para fins pessoais e recreativos, vedação de acesso a sites que não agreguem conhecimento profissional ou para o negócio.	**Concluído**
17	Criação de política de uso das estações de trabalho	Formatar política de utilização das estações de trabalho, visando à segurança das informações contidas nos computadores, em atendimento à LGPD.	Informática	1- Vedar a utilização de estação de trabalho de outro empregado sem a autorização da chefia e a devida comunicação à equipe de TI 2 - Configurar as permissões necessárias 3 - Tornar obrigatório o bloqueio da estações em caso de ausência do empregado 4 - Vedar a instalação de softwares e hardwares sem autorização/auxílio da equipe técnica. 5 - Vedar a realização de downloads de filmes, músicas, fotos em sites de pirataria, os quais são monitorados pela equipe de TI. 6 - Tornar obrigatório o armazenamento de todos os documentos no servidor de arquivos, para garantia de backup. 7 - Vedar a utilização de dispositivos pessoais de memória externa. 8 - Estabelecer as regras de uso de aplicativos de mensagens instantâneas (WhatsappWeb, Skype), em contas pessoais, corporativas, nas estações de trabalho. 9 - Estabelecer regras de bloqueio das portas USB dos computadores. 10 - Estabelecer regras de uso dos smartphones. 11 - Estabelecer regras de transferÊncia de arquivos.	**Concluído**
18	Criação de política de relação com terceiros	Escrever política de confidencialidade em relação às informações da empresa, a ser seguida pelos funcionários e em conformidade com a Classificação das Informações, com o objetivo de atender à LGPD.	Licitação e DPO	1 - Elaborar política determinando, dentre outros pontos que a empresa julgar pertinente, que as informações recebidas pelos empregados, para fins de prestação de serviços, são confidenciais e não devem ser repassadas a empregados não autorizados ou a terceiros 2 - Estabelecer diretrizes com o intuito de evitar a divulgação e utilização não autorizada das informações confidenciais da empresa	**Concluído**
19	Criação de política sobre documentação física e sustentabilidade	Elaborar política sobre utilização, impressão e acesso a documentos físicos, inclusive com viés de sustentabilidade, observando os preceitos da LGPD.	Comissão de Sustentabilidade	Elaborar política contendo diretrizes para gerir as atividades da empresa de forma sustentável, considerando fatores econômicos, sociais e ambientais	**Concluído**

Etapa 2 - Construção e Execução					
Nº	**Ação de melhoria**	**Motivo**	**Responsável**	**Atividades desenvolvidas**	
20	Criação de política de anonimização, bloqueio e eliminação de dados	Elaborar critérios e procedimentos para anonimização, bloqueio e exclusão dos dados pessoais tratados pelo cliente, atendendo aos requisitos impostos pela LGPD.	DPO e Informática	1 - Elaborar política contendo as diretrizes de anonimização, bloqueio e exclusão dos dados tratados pela empresa. 2 - A anonimização permite que não se identifique uma pessoa, a fim de restringir o tratamento das informações por pessoas não autorizadas e limitar a identificação do titular, dispensando o consentimento do titular dos dados. 3 - Estabelecer critério sobre o bloqueio de dados. 4 - Estabelecer critérios sobre a forma e periodicidade de eliminação dos dados tratados pela empresa, levando em conta os prazos previstos nas legislações aplicáveis	**Concluído**
21	Criação de plano de continuidade de negócios	Desenvolver plano de continuidade de negócios, em caso de paralisação dos serviços decorrente de sinistro, com atenção ao disposto na LGPD e à segurança de dados.	Comissão	O plano de continuidade mostra o caminho a seguir em caso de sinistros e indisponibilidade dos recursos de TI. A ISO 27001 A.17 mostra o aspectos da segurança da informação na gestão da continuidade do negócio. Recomenda-se a elaboração e implantação de documentação de um plano de continuidade para os recursos críticos e uma análise de riscos para ver os pontos mais críticos levando e conta a probabilidade de acontecer e impacto para empresa. Convém que a organização determine seus requisitos para a segurança da informação e a continuidade da gestão de segurança da informação em situações adversas, por exemplo, durante uma crise ou desastre. Sem o plano de continuidade para dar a direção a ser tomada em caso de crises ou desastre, a empresa pode perder todas as suas informações ou demorar um tempo inadequado para conseguir restabelecer todos os seus recursos imprescindíveis.	**Concluído**
22	Criação de política de controle de acesso aos usuários	Estabelecer critérios para configuração de estações de trabalho, com observância dos acessos necessários para desempenho das funções do empregado, conforme a LGPD.	Informática	De acordo com a ISO 27002: Controle de acessos Política de controle de acesso Controle Convém que uma política de controle de acesso seja estabelecida, documentada e analisada criticamente, baseada nos requisitos de segurança da informação e dos negócios. Diretrizes para implementação Convém que os proprietários dos ativos determinem regras apropriadas do controle de acesso, direitos de acesso e restrições para papéis específicos dos usuários acessarem seus ativos, com o nível de detalhe e o rigor dos controles que reflitam os riscos de segurança da informação associados. Convém que sejam considerados os controles de acesso lógico e físico (Ver 11) de forma conjunta. Convém que uma declaração nítida dos requisitos do negócio a serem atendidos pelo controle de acesso, seja fornecida aos usuários e provedores de serviços. Recomenda-se a utilização de um sistema de registro de incidentes para as solicitações de inclusão, exclusão, troca de função e perfil que mantenha o histórico e a aprovação do procedimento, por parte do solicitante.	**Concluído**
23	Criação de política de backup e restore	Redigir política de backup e restauração de dados que observe critérios de modo e periodicidade de cópia dos dados armazenados nos sistemas da empresa, visando ao atendimento da LGPD.	Informática	Elaborar política estabelecendo critérios que assegurem o acesso e a proteção das informações eletrônicas da empresa, contendo o modo e a periodicidade de cópia dos dados armazenados pelos sistemas computacionais.	**Concluído**
24	Revisão de política de gestão de riscos	Revisar política de gestão de riscos, com intuito de desenvolver e implementar melhorias das metodologias de gerenciamento dos riscos corporativos, visando à segurança dos dados utilizados pela empresa, conforme a LGPD.	DPO	1 - Revisar política contendo princípios e diretrizes da gestão de riscos, a fim de desenvolver, disseminar e implementar metodologias de gerenciamento de riscos corporativos e controles internos, para apoiar melhorias contínuas nos processos organizacionais, projetos e iniciativas estratégicas da empresa, contribuindo para o alcance dos objetivos estratégicos e cumprimento do propósito institucional. 2 - Deve conter a caracterização do ambiente interno, definição de objetivos, eventos de risco, avalização, respostas e priorização dos riscos, forma de controle e comunicação, dentre outros pontos que a empresa julgar relevante.	**Concluído**
25	Criação de política de BYOD	Produzir política com critérios para utilização de dispositivos móveis pessoais dos empregados, visando à segurança das informações repassadas por meio dos aparelhos e aplicativos, em atendimento à LGPD.	Informática	1 - Elaborar política estabelecendo critérios para o uso de dispositivos móveis pessoais dos empregados da empresa, nos ambientes internos e externos, para a prestação de serviços, bem como quais dispositivos são permitidos e de que forma. 2 - Estabelecer as regras de segurança que devem ser utilizadas como: recursos determinados pela TI, rede segura, armazenameto das informações, senhas e demais medidas de segurança	**Em andamento**
26	Criação de política de acesso remoto	Definir regras e procedimentos de segurança para acesso remoto ao ambiente de tecnologia da empresa que contenha dados e informações sigilosas, conforme LGPD.	Informática	1 - Elaborar política estabelecendo os procedimentos para o acesso remoto. 2 - O documento deve estar em conformidade com a política de segurança da informação. 3 - Estabelecer as situações de acesso remoto, controles e responsabilidades.	**Concluído**

Etapa 2 - Construção e Execução					
Nº	**Ação de melhoria**	**Motivo**	**Responsável**	**Atividades desenvolvidas**	
27	Criação de política de segurança cibernética	Elaborar os princípios e diretrizes de proteção das informações consideradas sensíveis da instituição e de seus clientes, visando a atender à LGPD.	Informática	1 - Elaborar política estabelecendo critérios para aplicar os princípios e diretrizes de proteção das informações consideradas sensíveis. 2 - Estabelecer os procedimentos para reduzir as vulnerabilidades. 3 - Estabelecer os procedimentos que devem ser seguidos pelos prestadores de serviço, fornecedores e empresas conveniadas. 4 - Classificação das informações de acordo com a confidencialidade, quem pode acessar as informações.	**Concluído**
28	Criação de política de tratamento incidentes	Estabelecer procedimento para tratamento de incidentes de segurança de informações pessoais, conforme definido na LGPD.	Informática	1 - Elaborar política estabelecendo regras e procedimentos de segurança para o registro de ocorrência de incidentes no ambiente de tecnologia e/ou analógico utilizado pela empresa 2 - Estabelecer os procedimentos que devem ser tomados no caso de incidentes que acarretem risco ou dano aos titulares, como será tratada a ocorrência (registro, comunicação à ANPD, emitir relatório, entre outras ações que a empresa entender adequada). 3 - Qual o tratamento após a solução definitiva do incidente.	**Concluído**
29	Criação de Política de Classificação das informações	Criar critérios para classificação das informações da empresa, com base no Anexo A.8.2 da ISO 27.001 e na LGPD.	Comissão	1 - Elaborar norma de classificação das informações que integrará a Política de Segurança da Informação da empresa e sujeitará todos os funcionários e terceiros a seguir as diretrizes. 2 - Deverá estabelecer a classificação das informações definidas no Anexo A.8.2 da ISO 27.001, que dispõe que seu objetivo é garantir que as informações recebam proteção em nível apropriado e de acordo com a sua importância junto à empresa. 3 - Estabelecer o grau de confidencialidade das informações, os prazo de restrição de acesso à informação, de quem é a competência da classificação, proteção e controle, reclassificação e reavaliação, rotulação da informação, dentre outras informações que a empresa entenda adequada.	**Concluído**
30	Restringir acesso dos usuários que não devem ter acesso, conforme o respectivo cargo e função	Revisar os acessos de todos usuários do sistema e corrigir as divergências.	Informática	1 - Delimitar os acessos de acordo com os cargos, funções e atividades exercidas, para que ninguém tenha acesso desnecessário a dados que não sejam pertinentes para a realização do trabalho ou não estejam anonimizados.	**Concluído**
31	Elaboração de modelos de resposta à solicitações da ANPD	Redigir modelo de resposta à solicitações da ANPD, estipulando as informações necessárias que o DPO deverá acrescentar, em observância à LGPD.	DPO	1 - O modelo de resposta deve conter o previsto no §1º do art.48. 2 - Deve explicar detalhadamente as medidas técnicas e administrativas (art. 46, LGPD) adotadas para reverter ou mitigar os efeitos do prejuízo, inclusive informando os prazos para cada uma das medidas. 3 - Descrever em detalhes a solução encontrada para o problema ou informar os motivos pelos quais não teve solução.	**Concluído**
32	Revisão de termo de sigilo e confidencialidade	Revisar termo de confidencialidade aos parceiros e empregados, estabelecendo punições pelo descumprimento, observando a LGPD	Comissão	1 - Revisar termo existente para evitar a divulgação e utilização não autorizada das informações confidenciais trocadas entre a empresa e parceiros/empregados. 2 - Estabelecer quais informações são confidenciais. 3 - De que forma a parte receptora poderá utilizar as informações confidenciais. 4 -Cláusula estabelecendo que a receptora se compromete a manter sigilo. 5 - Estabelecer sanções em caso de descumprimento, entre outras informações que a empresa entenda pertinentes.	**Concluído**
33	Elaboração de notificações aos terceiros/parceiros	Redigir as notificações para os parceiros, visando a identificar seu nível de adequação à LGPD e permitir a decisão quanto à continuidade da relação jurídica ou rescisão daqueles que apresentam grande vulnerabilidade.	Comissão	1 - O documento visa identificar o nível ou plano de ação para que a empresa esteja em compliance com a LGPD. 2 - Questionar sobre a conformidade da empresa com os requisitos impostos pela LGPD, quais políticas, medidas e boas práticas já estão implementadas na empresa. 3 - Se utilizam sistema rodando em nuvem. 4 - Se realizam testes sistemáticos de intrusão ou de acessos indevidos aos seus sistemas e ambientes. 5 - Se possuem Relatório de Impacto à Proteção de Dados Pessoais, conforme previsto no inciso XVII, do art. 5º, da referida Lei. 6 - Se possuem profissional com a função de Encarregado (DPO) para representá-los no que concerne à proteção de dados na empresa. 7 - Outras informações que a empresa julgar pertinentes.	**Concluído**
34	Elaboração de aditivo aos contratos dos prestadores de serviço	Elaborar os aditivos contratuais, com inclusão de cláusulas de sigilo e proteção de dados pessoais, conforme a LGPD.	Licitação e DPO	1 - Elaborar aditivos com cláusulas de sigilo e proteção de dados. 2 - Estabelecer que a parte concorda e consente que a empresa tome decisões referentes ao tratamento de seus dados pessoais, bem como realize o tratamento de seus dados pessoais. 3 - Listar os dados tratados e onde são cadastrados. 4 - Prazo para comunicar incidentes. 5 - Prazo do tratamento dos dados 6 - Outras informações que a empresa julgar pertinentes	**Concluído**

Etapa 2 - Construção e Execução					
Nº	**Ação de melhoria**	**Motivo**	**Responsável**	**Atividades desenvolvidas**	
35	Elaboração de termos de consentimento	Elaborar os termos de consentimento dos titulares de dados pessoais, conforme necessidade do cliente. Em especial referente ao tratamento de dados dos empregados relacionado a gestão de pessoas da empresa.	Comissão	1 - Elaborar termo de consentimento dos titulares de dados quando necessários, como para o envio de exames ao médico solicitantes. 2 - Termo de consentimento de uso de dados dos empregados, quais dados são tratados e para quais finalidades.	**Concluído**
36	Elaboração de modelo de revogação do consentimento	Criar modelo de termo de revogação do consentimento para o titular de dados pessoais, para atendimento da LGPD.	Comissão	Estabelecer quais dados serão excluídos e quais são necessários para fins de obrigações legais	**Concluído**
37	Elaborar termo de consentimento para tratar dados de crianças e adolescentes	Criar modelo de termo de consentimento para tratar dados de menores, de acordo com o estabelecido na LGPD	Comissão	O termo deve abordar a manifestação livre, informada e inequívoca pela qual o representante legal ou um dos pais do Titular dos Dados Pessoais concorda com o tratamento de seus dados pessoais para finalidade específica	**Concluído**
38	Política de Armazenamento de Dados, Documentos e Arquivos (PADDA)	Instituir a PADDA, de acordo com o estabelecido na LGPD	Comissão	A política deve estabelecer diretrizes para a implementação de repositórios arquivísticos digitais confiáveis para o arquivamento e manutenção de documentos arquivísticos fisicos e digitais em suas fases corrente, intermediária e permanente.	**Concluído**
39	Política de Privacidade em Eventos	Elaborar política sobre privacidade em eventos, observando os preceitos da LGPD.	Desenvolvimento Profissional	A política deve trazer diretrizes sobre os dados pessoais do usuário poderão ser utilizados pelo Sistema de Eventos para atender a atividades necessárias no fornecimento dos serviços relacionados ao evento em que o titular se cadastrou.	**Concluído**
40	Termo de Cessão de Direito e de Autorização de Uso de Imagem e Voz	Criar modelo de termo de consentimento para tratar imagem e voz, de acordo com o estabelecido na LGPD	Desenvolvimento Profissional	Elaborar termo em observância à Lei nº. 13.709/18 – Lei Geral de Proteção de Dados Pessoais e demais legislações correlatas aplicáveis à proteção de Dados Pessoais, Identificação Civil e Direito de Imagem e de Voz, na qualidade de titular dos direitos de autor da publicação.	**Concluído**

Etapa 3 - Monitoramento					
Nº	**Ação de melhoria**	**Motivo**	**Responsável**	**Atividades desenvolvidas**	
41	Acompanhar a execução das atividades das etapas anteriores.	Acompanhamento mensal	DPO	Acompanhamento realizado por meio do monitoramento do plano de ação e reuniões periódicas com a equipe envolvida nos processos.	**Concluído**
42	Gerar relatório de análise de riscos relacionados à LGPD	Acompanhamento contínuo	DPO	Preenchimento de planilha específica com os riscos relacionados à LGPD	**Concluído**
43	Realizar auditorias para verificar a conformidade das políticas e processos do CRCPR com a LGPD.	Acompamhamento Semestral	DPO	Utilizadas as sugestões de indicadores do guia do governo federal, com alterações de acordo com a realidade do CRCPR. Estabelecidos 5 indicadores com apuração semestral. A planilha de controle contém os campos: indicador, objetivo, fórmula do indicador, meta, fonte, frequência de apuração, registros e responsável.	**Concluído**
44	Criar e alimentar planilha com o registro de incidentes de segurança da informação.	Acompanhamento mensal	DPO	Envio de e-mail mensal aos gestores questionando sobre registro de incidentes de vazamento de dados pessoais. Informações da planilha a ser preenchida pelos gestores em caso de incidente: descrição dos incidentes ou eventos; informações e sistemas envolvidos; medidas técnicas e de segurança utilizadas para a proteção das informações; riscos relacionados ao incidente e medidas tomadas para mitigá-los a fim de evitar reincidências.	**Concluído**
45	Criação de módulo sobre segurança de dados para integração de novos funcionários	Apresentando conceitos-chave e a política da empresa sobre segurança de dados durante a integração, para garantir a completa integração dos novos funcionários, já de acordo com a cultura de proteção praticada pelo CRCPR	CRCPR deve definir	1 - Fornecer aos novos colaboradores acesso ao workshop de conscientização. 2 - Dar treinamento para todos os empregados sobre a cultura e políticas da empresa.	**Em andamento**