Plano de Gestão de Riscos

JULHO DE 2022

Comitê Gestor de Privacidade do SENAC AL

Nome	Setor	E-mail
Vagner de Gusmão Cavalcanti	Planejamento/Controladoria	vagner.cavalcanti@al.senac.br
Samuel Vasconcelos da Silva	TI	samuel.vasconcelos@al.senac.br
Felipe Dietschi Falcão	Contratos, Estoque e Licitação	felipe.falcao@al.senac.br
Diego de Souza Pinto	TI	diego.souza@al.senac.br
João Carlos Azarias de Oliveira	TI - Unidade Arapiraca	joao.oliveira@al.senac.br
Cristiane Calaça Correia Botelho	Marketing/Comunicação/Centrais de atendimento/Callcenter	cristiane.calaca@al.senac.br
Aline Baracho Wanderley de Oliveira	Ouvidoria	aline.baracho@al.senac.br
Aristóteles da Silva Oliveira	Gerência de Educação Profissional	aristoteles.oliveira@al.senac.br
Sheila Vieira de Melo	RH	sheila.vieira@al.senac.br
Rosimeire Guedes da Silva	Financeiro	rosimeire.guedes@al.senac.br

Equipe Técnica do Grupo ADX

Adriano Lima Head de Projetos	**Adgenison Nascimento** Head de Negócios
Gessica Alcântara Gestora de Projetos	**Hendrick Arcanjo** Consultor de Tecnologia
Laís Gomes Analista de Processos	**Saulo Santos** Advogado

Histórico de revisões			
Versão	**Data**	**Autor**	**Descrição**
1.0	29/07/2022	Grupo ADX	Elaboração do documento

SUMÁRIO

ÍNDICE DE FIGURAS

1 – OBJETIVO

O objetivo deste documento é estabelecer a metodologia de gestão de riscos, no âmbito do SENAC AL, para execução dos planos de ações necessários para atender às exigências legais previstas na Lei Geral de Proteção de Dados (LGPD), no tocante a gestão de segurança da informação e privacidade.

2 - REFERÊNCIAS

- Norma ABNT NBR ISO 31000:2018 – Gestão de Riscos: Princípios e Diretrizes;
- Lei nº 13.709 – Lei Geral de Proteção de Dados;

3 – CONCEITOS IMPORTANTES

I – Processo: conjunto de ações e atividades inter-relacionadas, que são executadas para alcançar produto, resultado ou serviço predefinido;

II – Método de priorização de processos: classificação de processos baseada em avaliação qualitativa e quantitativa, visando ao estabelecimento de prazos para a realização de gerenciamento de riscos;

III – Governança: combinação de processos e estruturas implantadas pela alta administração da organização, para informar, dirigir, administrar, avaliar e monitorar atividades organizacionais, com o intuito de alcançar os objetivos e prestar contas dessas atividades para a sociedade;

IV – Objetivo organizacional: situação que se deseja alcançar de forma a se evidenciar êxito no cumprimento da missão e no atingimento da visão de futuro da organização;

V – Meta: alvo ou propósito com que se define um objetivo a ser alcançado;

VI - Procedimentos de controle: políticas e procedimentos estabelecidos para enfrentar os riscos e alcançar os objetivos institucionais;

VII - Procedimentos de controles internos: procedimentos que a Empresa executa para o tratamento do risco, projetados para lidar com o nível de incerteza previamente identificado;

VIII – Risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos. O risco é medido em termos de impacto e de probabilidade;

IX - Risco inerente: risco a que uma organização está exposta após a implementação de medidas de controle que possam reduzir a probabilidade de sua ocorrência ou seu impacto;

X – Risco residual: risco a que uma organização está exposta após a implementação de medidas de controle para o tratamento do risco;

XI - Riscos de imagem ou reputação: eventos que podem comprometer a confiança da sociedade ou de parceiros, de clientes ou de fornecedores, em relação à capacidade da Empresa em cumprir sua missão institucional;

XII - Riscos financeiros ou orçamentários: eventos que podem comprometer a capacidade institucional de contar com os recursos orçamentários e financeiros necessários à realização de suas atividades, ou eventos que possam comprometer a própria execução orçamentária;

XIII - Riscos legais: eventos derivados de alterações legislativas ou normativas que podem comprometer as atividades da Empresa;

XIV - Riscos operacionais: eventos que podem comprometer as atividades institucionais, normalmente associados a falhas, deficiência ou inadequação de processos internos, pessoas, infraestrutura e sistemas;

XV - Nível de risco: magnitude de um risco, expressa em termos da combinação de suas consequências e probabilidades de ocorrência;

XVI - Tolerância ao risco: nível de variação aceitável quanto à realização dos objetivos;

XVII - Tratamento do risco: processo de estipular uma resposta aos riscos;

XVIII – Apetite ao risco: nível de risco que uma organização está disposta a aceitar;

XIX - Categoria de riscos: classificação dos tipos de riscos definidos pela Empresa que podem afetar o alcance de seus objetivos estratégicos, observadas as características de sua área de atuação e as particularidades do setor público;

XX – Gestão de riscos: é o conjunto de atividades coordenadas, estruturado definindo claramente os princípios, objetivos, estrutura, competências e processo para dirigir e controlar em uma organização no que se refere a riscos necessário para gerenciar riscos eficazmente;

XXII - Processo de gestão de riscos: aplicação sistemática de políticas, procedimentos e práticas de gestão para as atividades de identificação, avaliação, tratamento e monitoramento de riscos, bem como de comunicação com partes interessadas em assuntos relacionados a risco;

XXIII - Proprietário do risco: pessoa ou unidade/setor com a responsabilidade e a autoridade para gerenciar o risco;

XXIV - Probabilidade: possibilidade/chance de ocorrência de um evento;

XXV - Resposta ao risco: qualquer ação adotada para lidar com risco, podendo consistir em: a) aceitar o risco por uma escolha consciente; b) transferir ou compartilhar o risco a outra parte; c) evitar o risco pela decisão de não iniciar ou descontinuar a atividade que dá origem ao risco; ou mitigar ou reduzir o risco diminuindo sua probabilidade de ocorrência ou minimizando suas consequências;

XXVI - Identificação de risco: processo de busca, reconhecimento e descrição de riscos, que envolve a identificação de suas fontes, causas e consequências potenciais, podendo envolver dados históricos, análises teóricas, opiniões de pessoas informadas e de especialistas, e as necessidades das partes interessadas;

XXVII - Incerteza: incapacidade de saber com antecedência a real probabilidade ou o impacto de eventos futuros;

XXVIII - Impacto: efeito resultante da ocorrência do evento;

XXIX - Mensuração de risco: processo que visa estimar a importância de um risco e calcular a probabilidade de sua ocorrência;

XXX - Monitoramento: componente do controle interno que permite avaliar a qualidade do sistema de controle interno ao longo do tempo;

XXXI – Controles internos da gestão: processo que engloba o conjunto de regras, procedimentos, diretrizes, protocolo, rotinas de sistemas informatizados, conferências e trâmites de documentos e informações, entre outros, operacionalizados de forma integrada, destinados a enfrentar os riscos e fornecer segurança razoável de que os objetivos organizacionais serão alcançados;

XXXII – Controle: medida aplicada pela organização para tratar os riscos, aumentando a probabilidade de que os objetivos e as metas organizacionais estabelecidas sejam alcançados;

- **XXXIII - Programa de integridade**: conjunto estruturado de medidas institucionais voltadas para a prevenção, detecção, punição e remediação de fraudes e atos de corrupção, em apoio à boa governança;
- **XXXIV - Risco à integridade**: vulnerabilidades que podem favorecer ou facilitar a ocorrência de práticas de corrupção, fraudes, irregularidades e/ou desvios éticos e de conduta, podendo comprometer os objetivos institucionais.

3 – Plano de Gestão de Riscos

Riscos são eventos ou condições incertas que, se ocorrerem, geram efeitos positivos ou negativos sobre o negócio.

O objetivo deste plano é fornecer aos responsáveis pelo tratamento de dados pessoais uma orientação para identificar lacunas de segurança da informação e de privacidade sobre os sistemas, contratos e processos da instituição.

Ao longo do plano será discorrido sobre o embasamento teórico utilizado, organização dos temas segurança da informação e privacidade nos controles propostos e a avaliação dos riscos de segurança da informação e privacidade. Todas essas etapas não apenas servem como uma oportunidade de identificação de lacunas como também são insumos para a elaboração dos Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), item obrigatório para o processo de adequação à LGPD.

A avaliação de riscos traz diversos benefícios para a empresa. Um resumo desses benefícios por ser visto na **Figura 1**.

Figura 1 - Benefícios da avaliação de riscos.

4 – ISO 31000

A ISO 31000 é a norma internacional para gestão de risco. Ao fornecer princípios e diretivas abrangentes, esta norma ajuda organizações em suas análises e avaliações de riscos. Sendo em uma empresa pública, privada ou comunitária, a ISO 31000 poderá contribuir bastante, pois ela se aplica à maioria das atividades de negócios, incluindo planejamento, operações de gestão e processos de comunicação.

De maneira alinhada com outros padrões internacionais de gerenciamento de riscos, os princípios e linhas gerais da norma ISO 31000 definem o risco como incerteza quanto aos objetivos, tendo como efeito, desvios em relação ao que foi planejado. Dessa forma, a gestão de riscos compreende um conjunto de ações realizadas de maneira coordenada no que tange as questões relacionadas ao controle dos riscos. Com o objetivo de melhor ilustrar a interação entre os processos de risco para a norma ISO 31000 a **Figura 2** apresenta todos os processos, as suas relações e fluxo de informações que são representados por setas que interligam cada fase do processo de gerenciamento de riscos.

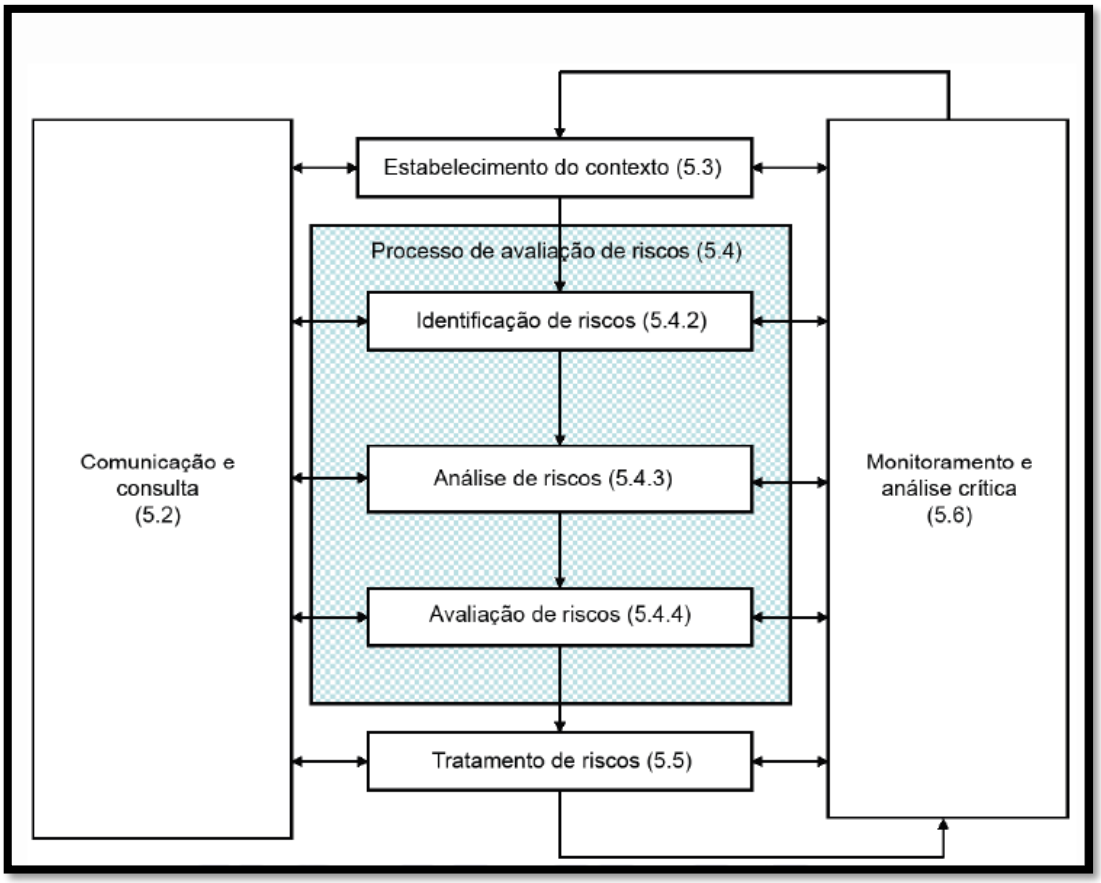

Figura 2 - Processo de gestão de riscos (ABNT NBR ISO/IEC 31000:2018).

De acordo com a ISO 31000 o fluxo dos processos de gestão de riscos começa com o plano de comunicação e consulta às partes interessadas em estágio inicial do projeto, onde questões relativas aos riscos são abordadas. Como a comunicação no ambiente corporativo acontece durante todo o ciclo de vida da informação, o sucesso na estruturação de bons

mecanismos de comunicação irá auxiliar no estabelecimento do contexto, envolvimento das partes interessadas, identificação de riscos e desenvolvimento de respostas.

Na etapa de desenvolvimento do contexto, o objetivo é traçar as metas do gerenciamento de riscos, definir o que será levado em consideração, tanto internamente, quanto externamente e quais as inter-relações existentes. Nessa linha de pensamento, a incorporação de parâmetros externos no gerenciamento de riscos contribui para que seja assegurado que os pontos de atenção das partes interessadas externas estão sendo considerados no processo, além de requisitos legais e regulatórios, ambiente cultural, político, legal, financeiro, tecnológico, regional, internacional, dentre outros.

Pela ótica interna, o processo de gestão de riscos deve estar alinhado à estratégia da organização, cultura, processos, governança e políticas corporativas, uma vez que estes fatores influenciam a maneira que a empresa gerencia os riscos . Dessa forma, os processos de gerenciamento de riscos são incorporados ao contexto da organização com foco na ampliação da capacidade da empresa em reconhecer oportunidades, garantindo maior comprometimento das partes interessadas, e estabelecimento de um ambiente de credibilidade, confiança e agregação de valor. Em linhas gerais, no estabelecimento do contexto são justificados os recursos que serão empregados para a realização dos processos de gestão de riscos através do estabelecimento de objetivos claros, definição de responsabilidades, abrangência das atividades de gestão de riscos, metodologia, escolha dos indicadores de desempenho, de maneira que a estratégia escolhida para o gerenciamento dos riscos esteja alinhada ao cenário, objetivos organizacionais e necessidades dos processos. Neste sentido, os critérios de riscos são definidos para serem utilizados para avaliar a significância do risco para a organização. Estes critérios poderão ser derivados de marcos regulatórios, requisitos legais e/ou políticas da organização.

O próximo processo abordado pelo referido padrão é o de avaliação dos riscos. Nesta etapa, os riscos são identificados e listados tendo como referência eventos com potencial para afetar o negócio da empresa, tanto positivamente como negativamente. Um ponto de atenção desta fase é que a identificação deverá ser o mais abrangente possível, tendo em vista que os riscos que não forem identificados na fase de identificação não serão considerados nas fases de análise posteriores.

Com o avanço na identificação dos riscos é iniciado o processo de avaliação, onde o objetivo é auxiliar o processo de tomada de decisão sobre os riscos que necessitarão de tratamento. A decisão sobre aplicar respostas aos riscos ou simplesmente manter os controles existentes irá depender do posicionamento da organização em relação aos riscos, limites de tolerância e demais critérios estabelecidos durante a fase de planejamento.

Após a análise dos riscos e seleção dos que irão receber tratamento, são desenvolvidos os planos de resposta contendo o detalhamento das opções consideradas, os benefícios esperados, pessoas responsáveis pela aprovação e execução das ações e os critérios de medição de desempenho. Como parte do processo de gestão de riscos, a fase de monitoramento e análise crítica é a etapa onde são estabelecidas as vigilâncias regulares e checagem dos riscos identificados e analisados nas fases anteriores. O objetivo desta etapa é verificar se os controles continuam eficazes, coletar informações que possam contribuir para o melhoramento dos processos de gestão de riscos, identificar nos riscos, detectar mudanças no cenário e implementar os planos de tratamento dos riscos.

Por fim, com o objetivo de tornar a análise de riscos uma atividade rastreável e com aproveitamento dos registros como mecanismos para a melhoria contínua dos métodos, processos e ferramentas, são criados os registros do processo de gestão de riscos. Estes, por sua vez poderão ser consultados por outros projetos com convergências de características, o que traz benefício para a organização e melhora o desempenho e maturidade da governança corporativa a partir do gerenciamento de riscos.

1 – Estabelecimento do Contexto

O contexto desse plano de gestão de risco é especificamente relacionado aos requisitos de adequação do SENAC AL à LGPD. Todos os temas aqui tratados terão relação direta com os controles necessários para adequação da empresa dentro da esfera jurídica, sempre privilegiando a segurança da informação e a privacidade.

2 – Identificação dos riscos

Para a identificação dos riscos, foi realizado um diagnóstico completo dentro das instalações da do SENAC AL, usando ferramentas como Workshops, entrevistas individuais, desenhos de processos, observações em campo e auditorias. Todas essas ações foram conduzidas por profissionais experientes em diversas áreas como proteção de dados, tecnologia, segurança da informação, jurídica, engenharia de produção e gestão de processos de negócios.

3 – Análise de riscos

Para a mensuração do impacto do risco no processo é necessário que sejam analisados os seguintes critérios:

- **Critério de proporcionalidade** (nº de titulares impactados ou envolvidos)
  - ✓ Classificação 1 - quando são impactados/envolvidos entre 01 e 99 titulares;
  - ✓ Classificação 2 - quando são impactados/envolvidos entre 100 e 999 titulares;
  - ✓ Classificação 3 - quando são impactados/envolvidos mais de 1000 titulares.

- **Critério de ambiente organizacional dos envolvidos**
  - ✓ Classificação 1 - risco interno (envolve o acesso ao dado de forma indevida por colaboradores da organização (controlador));
  - ✓ Classificação 2 - risco externo médio (envolve o acesso ao dado pessoal de forma indevida por operadores, clientes, fornecedores ou outro ator externo à organização);
  - ✓ Classificação 3 - risco externo grave (envolve o acesso ao dado pessoal sensível de forma indevida por operadores, clientes, fornecedores ou outro ator externo à organização).

- **Critério de localização do tratamento de dados**

  - ✓ Classificação 1 - dado tratado dentro da organização;
  - ✓ Classificação 2 - o tratamento dos dados é realizado tanto internamente quanto externamente à organização;
  - ✓ Classificação 3 - o tratamento dos dados é realizado externamente à organização.

- **Critério de envolvimento de dados de crianças e adolescentes**

  - ✓ Classificação 2 - há o tratamento de dados pessoais de crianças e adolescentes;
  - ✓ Classificação 3 - há o tratamento de pelo menos um dado pessoal sensível de crianças e adolescentes.

- **Critério de classificação do dado pessoal sensível**

  - ✓ Sempre que houver o tratamento de dado pessoal sensível no processo, a classificação deve ser no mínimo 2.

OBS: Quando o processo se enquadrar em mais de um dos critérios de classificação, sempre adotar o critério que resulte em maior impacto.

Para a mensuração da probabilidade de ocorrência do risco, deve-se considerar o esforço necessário para a materialização do risco:

- ✓ Classificação 1 - Muito esforço (ex.: acessar o sistema, procurar o cliente e correlacionar informações);
- ✓ Classificação 2 - Médio esforço (ex.: acessar o sistema e procurar o cliente);

- ✓ Classificação 3 - Pouco esforço (ex.: já possuir os dados).

Os riscos identificados possuem um atributo chamado de criticidade do risco. A criticidade é o resultado da multiplicação de probabilidade x impacto. O resultado dessa operação possui valores possíveis de 1 a 9. Dessa forma os riscos se enquadram de acordo com a matriz a seguir:

Probabilidade	Valor
Baixa	1
Média	2
Alta	3

Impacto	Valor
Baixo	1
Médio	2
Alto	3

Figura 3 - Probabilidade X Impacto dos riscos.

Foi definido que os riscos de exposição inferior a 3 possuem exposição baixa, entre 4 e 5 possuem exposição média e acima de 5 exposição alta. Os riscos serão classificados por prioridade e impacto, de acordo com o gráfico a seguir.

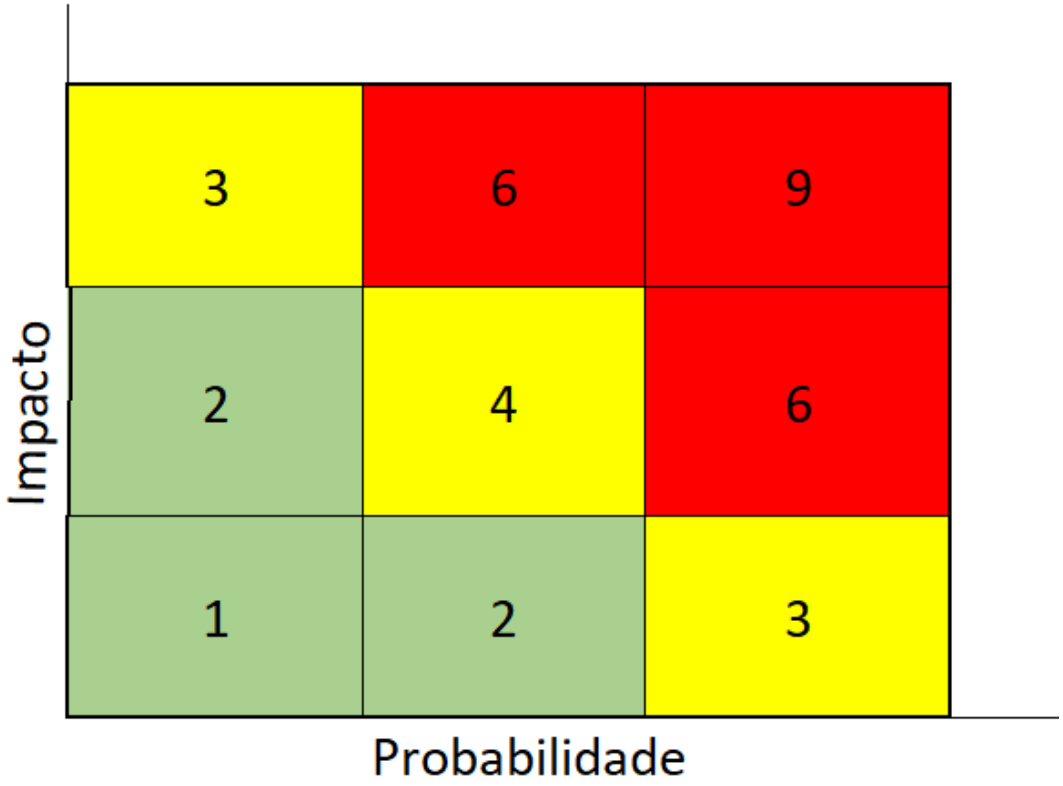

Figura 4 - Matriz de avaliação de riscos.

4 - Avaliação dos riscos de segurança e privacidade

A avaliação dos riscos de segurança e privacidade foi estruturado de modo a facilitar a reprodução e a adaptação do método proposto. O plano de respostas ao risco será apresentado em forma de um plano de ação e esse plano pode pertencer a três dimensões. As dimensões agrupam os controles, de forma didática, em três contextos distintos: Segurança da Informação, Jurídico ou Organizacional.

4.1 Contexto da Segurança da Informação

Nesta dimensão são avaliados controles que tratam de aspectos relacionados à confidencialidade, integridade e disponibilidade dos ativos críticos da organização, características de ambiente que expandem a análise, mas indispensável para identificar o estado atual da segurança e privacidade na organização responsável pelo tratamento de dados pessoais. A análise dos sistemas tem alicerce no processo de Security-by-Design , ou seja, os controles de segurança propostos visam incorporar a segurança da informação durante todo o ciclo de vida do sistema, consequentemente auxiliam a redução da superfície de ataque para vulnerabilidades de sistema. Exemplos de controles previstos nessa dimensão são: Implementação de políticas de backup, realização de análise de vulnerabilidades, implantação de soluções para gestão corporativa de antivírus, redundância de firewalls etc.

4.2 Contexto Jurídico

Essa dimensão analisa os riscos existentes nos fluxos de processos desenhados para os tratamentos de dados pessoais, em função dos requisitos legais descritos no texto da LGPD. Os controles visam garantir que nenhum item obrigatório previsto pela lei foi deixado de ser implementado. Exemplos de controles previstos nessa dimensão são: Definição de cada base legal associada aos processos mapeados, nomeação do DPO, disponibilização dos contatos do DPO no site da empresa, implantação do processo de atendimento aos direitos dos titulares etc.

4.3 Contexto Organizacional

Os controles presentes nesta dimensão estão relacionados ao modo como os processos funcionam para tender os requisitos da LGPD. Pode ser necessário alterar as atividades de um processo para atendimento a um requisito legal ou de segurança. Exemplos dessa categoria são: Necessidade de criar um procedimento para padronizar a forma como

uma tarefa é executada, necessidade de criar um novo processo para atender a um requisito da LGPD etc.

Para cada risco identificado é adotada uma estratégia de tratamento e resposta. As estratégias possíveis de respostas às ameaças e/ou oportunidades são:

- **Aceitar:** Não fazer nada previamente. Os riscos se enquadram nos critérios de aceitação e ficam em observação, sem ação pré-definida. Pode envolver criar um plano de contingência, para o caso de o risco ocorrer (Aceitação ativa);
- **Eliminar:** Eliminar a ameaça destruindo a sua causa. Esse é o critério a ser utilizado para riscos não toleráveis pela organização.
- **Mitigar:** Minimizar os impactos negativos e a probabilidade de o risco ocorrer, reduzindo sua criticidade e tornando-o um risco menor.
- **Transferir:** Tornar outra parte responsável pelo risco, como por exemplo, contratando seguros ou terceirizando trabalhos.
- **Explorar:** Em caso de oportunidades (riscos positivos) determinar ações para maximizar as possibilidades de um risco ocorrer e otimizar seu impacto caso ele ocorra.

Após a realização da análise de riscos em todos os processos mapeados, foi feita a definição de seus respectivos controles de segurança da informação, jurídicos ou organizacionais, para adequação à LGPD. Cada controle pode atuar de maneira diferente em relação a um determinado risco: podem contribuir para a prevenção do risco, para sua mitigação, ou ambos ao mesmo tempo. Controles de prevenção atuam na redução da probabilidade da ocorrência do risco e controles de mitigação atuam na redução do impacto do risco. Foi gerado o gráfico como resumo dos riscos e controles identificados em cada setor.

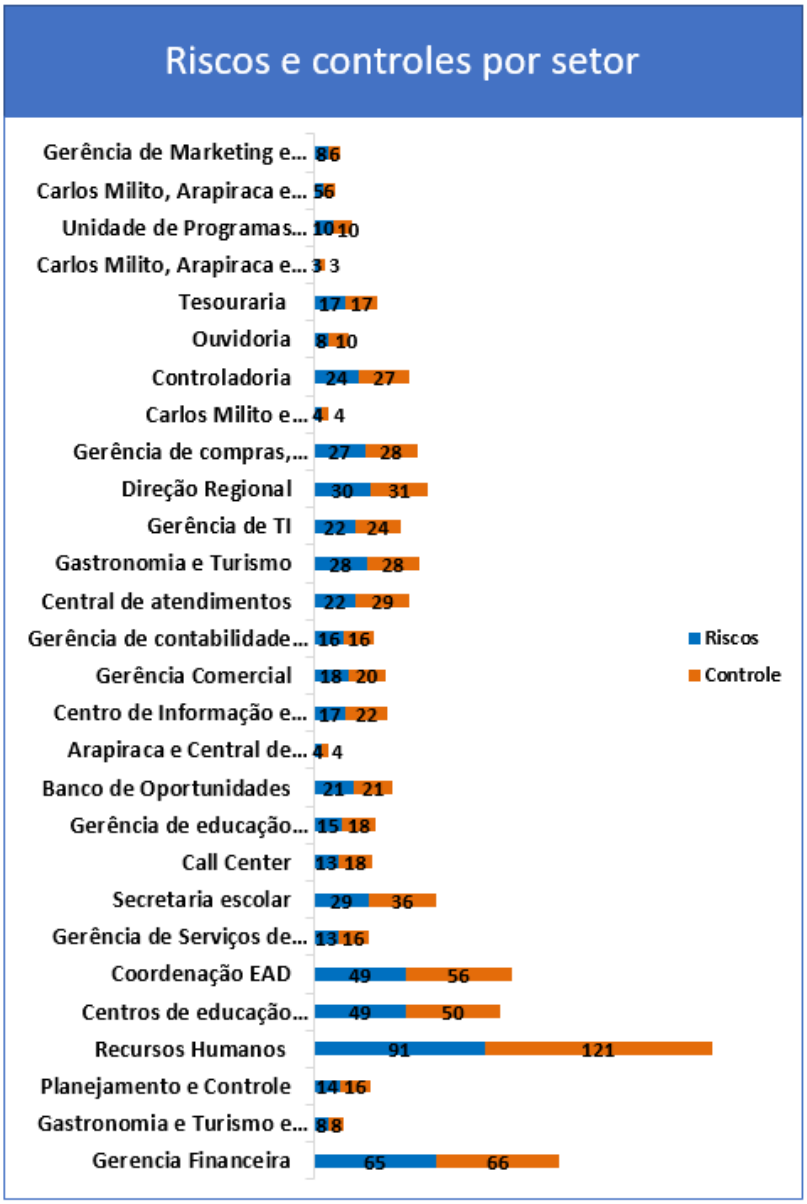

Figura 5 - Nº de riscos e controles por setor.

Todos os riscos identificados foram associados aos processos que tratam dados pessoais dentro do SENAC AL, transferindo as suas criticidades os fluxos de dados pessoais existentes na organização. A tabela a seguir agrupa os processos de acordo com cada faixa de criticidade definidas no plano de gerenciamento de riscos.

Criticidade 9
Criticidade 6
RH 13 - Demitir colaborador
COORD EAD 03 - Matricular alunos na modalidade FIC

RH 03 - Encaminhar e marcar exame admissional do colaborador
RH 07 - Gerenciar os exames de saúde ocupacional
RH 10 - Registrar e realizar manutenção do ponto
Criticidade 4
CEP GT E UPS 01 - Gerenciar documentos enviados ao RH
COORD EAD 07 - Acompanhar prática profissional do programa de aprendizagem
RH 05 - Integrar colaboradores
Call center 03 - Captar leads
BOP 02 - Realizar matrícula por convênio social
CEP Arapiraca e Central 01 - Realizar a matrícula de alunos
CEP GT e UPS 02 - Gerenciar documentos enviados ao setor Financeiro
RH 02 - Admitir colaboradores
Secretaria 01 - Gerenciar o arquivo físico
RH 06 - Avaliar desempenho do colaborador
COORD EAD 04 - Viabilizar a criação do código validador dos alunos dos cursos tec
GETI 01 - Criar acesso aos sistemas
COORD EAD 01 - Coletar dados para matrícula de alunos em cursos técnicos EAD - PSG
BOP 03 - Realizar controle de requerimento
CEP CM e GT 01 - Contratar serviços
Ouvidoria 01 - Gerenciar o canal de ouvidoria
CEP GT 02 - Realizar matrícula de alunos
RH 12 - Realizar processamento Férias
Controladoria 02 - Atender fiscalização contínua do TCU
BOP 05 - Elaborar relatórios gerenciais
Secretaria 03 - Cadastrar turmas e alunos no SISTEC
COORD EAD 10 - Acompanhar emissão de diplomas dos cursos técnicos
Central de atendimento 01 - Atender solicitação de alunos
CIC 03 - Cadastrar alunos na plataforma digital
RH 11 - Elaborar folha de Pagamento
CEPs 09 - Realizar planejamento de execução do curso
CEP GT 01 -Comunicar início de turma para instrutores ou convidados
RH 08 - Gerenciar benefícios
RH 01 - Recrutar novos colaboradores
GEP 02 - Emitir planilha de dados dos alunos
Central de atendimento 04 - Realizar matrícula in company ou convênio
COORD EAD 02 - Fornecer relatórios dos cursos realizados pelo EAD
RH 04 - Cadastrar colaborador
Secretaria 06 - Coletar dados para o censo escolar e sistema censo básico
UPS 01 - Realizar matrícula dos alunos
Call center 02 - Atender solicitações
Central de atendimento 03 - Abrir e fechar caixa
CEPs 05 - Aprovar informações para encerramento de produção mensal
GETI 05 - Gerar relatórios para outros setores
Criticidade 3
GETI 02 - Atender chamados de TI

Controladoria 04 - Realizar auditoria interna
GMAC 01 - Produzir materiais para divulgação.
GETI 04 - Realizar backup
Criticidade 2
GPC 01 - Realizar o cadastro no sistema Qualiex
COORD EAD 05 - Responder demandas do Fale Conosco e ouvidoria
COORD EAD 09 - Acompanhar o processo de matrícula dos alunos PROUNI
BOP 01 - Receber currículo para cadastro no BOP
Central de atendimento 05 - Emitir declarações para aluno
GFI 08 - Monitorar inadimplências.
Controladoria 01 - Realizar auditoria do conselho fiscal
CEPs 04 - Receber atestado e declarações de alunos
DR 01 - Colher dados para a auditoria interna.
BOP 04 - Atender solicitações de empresas de recrutamento
Ouvidoria 02 - Gerenciar o Fale Conosco
Secretaria 07 - Elaborar ementário escolar
RH 09 - Treinar e Desenvolver colaborador
Call center 01 - Atender solicitação de reserva de vagas e demandas
UPS 02 - Realizar parcerias através de convênios
DR 02 - Responder notificação judicial.
GCELC 03 - Realizar requisição de pedido de compra
GFI 06 - Recolher imposto de renda de aluguéis.
CIC 02 - Realizar backup
DR 04 - Compartilhar arquivos via Google Drive ou E-mail.
GFI 02 - Realizar pagamentos - Educação corporativa.
Criticidade 1
GFI 04 - Pagar NF ou fatura de pessoa jurídica.
CEPs 08 - Gerenciar grupo da turma em redes sociais e ambiente virtual
CEPs 01 - Elaborar folha de pagamento
GSAI 02 - Realizar o controle de contratos
GFI 09 - Realizar fechamento de movimentação financeira
Secretaria 04 - Emitir diploma, certificados e histórico escolar dos alunos
GFI 10 - Emitir notas fiscais de serviços.
GEP 03 - Participar das competições SENAC
CIC 01 - Cadastrar alunos e colaboradores na biblioteca
Gerência comercial 01 - Elaborar proposta ou projeto comercial
GECOR 01 - Elaborar o balancete
CEPs 07 - Enviar dados de carga horária de instrutores para pagamento
GPC 02 - Receber a produção institucional (GEP)
Central de atendimento 02 - Realizar matrícula de alunos via web
CEP GT 05 - Realizar avaliações institucionais
GFI 07 - Atender solicitações de alunos.
CEPs 02 - Gerenciar avaliação de alunos
COORD EAD 06 - Acompanhar Processos de Inscrição e Matrícula dos Ciclos Ativos
DR 05 - Divulgar documentos norteadores na intranet.

CIC 04 - Realizar empréstismos e devoluções de livros
GCELC 01 - Realizar Processo Licitatórios - Fase Interna
CEPs 03 - Realizar acompanhamento de matrículas
Gerência comercial 02 - Estabelecer parceria com convênio
CEP GT 03 - Receber equipamentos e utensílios
GFI 01 - Realizar pagamento das notas fiscais de serviço - PF.
SETES 03 - Reapresentar pagamento de devolução.
GCELC 02 - Realizar Processo Licitatórios - Fase externa
GFI 05 - Realizar pagamento de devolução.
GPC 03 - Enviar dados de alunos para o DN para realização de pesquisa
SETES 01 - Realizar fechamento de caixa.
Secretaria 05 - Enviar dados de aluno ao Bem legal
GEP 01 - Capacitar colaboradores
GETI 03 - Criar login de fornecedores na rede virtual
CEP CM, Arapiraca E UPS 01 - Realizar acompanhamento pedagógico
COORD EAD 08 - Receber relatório de resultado de seleção de estágio
SETES 02 - Agendar pagamentos de boletos e depósitos
CEPs 06 - Alocar instrutores e coordenadores nas turmas
GCELC 05 - Realizar a gestão contratual.
Secretaria 02 - Realizar cronograma de visita aos postos avançados e Arapiraca
GSAI 01 - Realizar o controle de acesso às unidades
Gerência comercial 03 - Visitar e prospectar clientes
DR 03 - Encaminhar demandas dos planos diretores.
CEP GT 06 - Realizar acompanhamento pedagógico
CEP CM, Arapiraca e GT 01 - Elaborar termo de compromisso para estágio
GFI 03 - Realizar pagamentos - Diárias
COORD EAD 11 - Acompanhar situação dos alunos dos cursos téc com documentação pendente
GCELC 04 - Elaborar contrato ou ARP
CEP GT 04 - Enviar dados de seguro
GECOR 03 - Enviar declarações para órgãos fiscais
GSAI 03 - Entregar correspondência
Secretaria 08 - Emitir certidões
CEPs 10 - Gerenciar frequência de aluno
GECOR 02 - Elaborar o balanço anual
Controladoria 03 - Enviar dados estratégicos para o portal da transparência
Controladoria 05 - Elaborar relatórios de gestão

Tabela 1 - Processos por criticidade.

O plano de gerenciamento dos riscos foi elaborado tendo como base a análise do ambiente e suas necessidades. Para cada risco levantado e priorizado foram calculados a categoria, probabilidade, impacto e exposição. Em seguida foram definidas as medidas preventivas e/ou de contingência. A tabela a seguir descreve cada item avaliado no plano de gerenciamento de riscos:

ITEM	DESCRIÇÃO
ID	Identificador do processo.
Setor	Setor responsável pelo processo.
Processo	Nome do processo.
Riscos	Descritivo dos riscos.
Probabilidade (P)	Probabilidade estimada de um risco ocorrer.
Impacto (I)	Impacto estimado se um risco ocorrer.
Criticidade (C)	Probabilidade multiplicada pelo Impacto.
Resposta ao risco	Atitude a ser tomada em relação ao risco.
Controles de segurança	Controles aplicados para garantir a estratégia de tratamento do risco.

Tabela 2 – Informações do plano de gestão de riscos.

Segue abaixo a tabela com os riscos e o respectivo plano de tratamento:

Nome do processo	Risco	Controle	Probabilidade	Impacto	Criticidade
GFI 04 - Pagar NF ou fatura de pessoa jurídica.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Envio de documentos em via física	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Recebimento de documentos por meio digital [Organizacional]	1	1	1

CEP GT E UPS 01 - Gerenciar documentos enviados ao RH	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Uso de formulário e documentos em papel	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Envio de documentos por meio digital [Organizacional]	2	2	4
GPC 01 - Realizar o cadastro no sistema Qualiex	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	1	2

RH 13 - Demitir colaborador	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Uso de formulário e documentos em papel ; Exclusão acidental dos dados ou problemas nos meios de armazenamento; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Utilização de Formulários Digitais [Organizacional]; Digitalização dos documentos evitando envio físico dos mesmos [Organizacional]; Revisar Política de Backup [Segurança da Informação]; Implementar medidas de segurança física e do ambiente [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	3	6
CEPs 08 - Gerenciar grupo da turma em redes sociais e ambiente virtual	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Envio de Dados por Whatsapp	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Informar os titulares da possibilidade de compartilhamento dos dados com este operador [Jurídico]; Não utilizar o celular pessoal do colaborador no processo [Organizacional]; Não enviar dados pessoais dos alunos via whatsapp [Segurança da Informação]	1	1	1

CEPs 01 - Elaborar folha de pagamento	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
COORD EAD 07 - Acompanhar prática profissional do programa de aprendizagem	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Envio de Dados por Whatsapp; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Não enviar dados pessoais dos alunos via whatsapp [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	2	4

GSAI 02 - Realizar o controle de contratos	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
GFI 09 - Realizar fechamento de movimentação financeira	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Uso de formulário e documentos em papel	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Digitalização do processo [Segurança da Informação]	1	1	1

RH 05 - Integrar colaboradores	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Exclusão acidental dos dados ou problemas nos meios de armazenamento; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Revisar Política de Backup [Segurança da Informação]; Implementar medidas de segurança física e do ambiente [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	2	4
Secretaria 04 - Emitir diploma, certificados e histórico escolar dos alunos	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar	1	1	1

		rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]			
GFI 10 - Emitir notas fiscais de serviços.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	1	1	1
Call center 03 - Captar leads	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

GEP 03 - Participar das competições SENAC	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
BOP 02 - Realizar matrícula por convênio social	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
CEP Arapiraca e Central 01 - Realizar a matrícula de alunos	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

CIC 01 - Cadastrar alunos e colaboradores na biblioteca	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
CEP GT e UPS 02 - Gerenciar documentos enviados ao setor Financeiro	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
RH 02 - Admitir colaboradores	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Exclusão acidental dos dados ou problemas nos meios de armazenamento; Não há procedimento estabelecido para o descarte dos dados	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Revisar Política de Backup [Segurança da Informação];	2	2	4

	do sistema após o atingimento da finalidade	Implementar medidas de segurança física e do ambiente [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]			
Gerência comercial 01 - Elaborar proposta ou projeto comercial	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
Secretaria 01 - Gerenciar o arquivo físico	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

GECOR 01 - Elaborar o balancete	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
CEPs 07 - Enviar dados de carga horária de instrutores para pagamento	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
GPC 02 - Receber a produção institucional (GEP)	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo	1	1	1

		para o descarte de dados após o fim da finalidade de tratamento [Organizacional]			
COORD EAD 05 - Responder demandas do Fale Conosco e ouvidoria	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]	1	2	2
Central de atendimento 02 - Realizar matrícula de alunos via web	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1

COORD EAD 09 - Acompanhar o processo de matrícula dos alunos PROUNI	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	2	2
CEP GT 05 - Realizar avaliações institucionais	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
RH 06 - Avaliar desempenho do colaborador	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Exclusão acidental dos dados ou problemas nos meios de armazenamento; Não há procedimento estabelecido para o descarte dos dados	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Revisar Política de Backup [Segurança da Informação]; Implementar medidas de segurança física e do	2	2	4

	do sistema após o atingimento da finalidade	ambiente [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]			
GFI 07 - Atender solicitações de alunos.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Recebimento de documentos físicos; Demais regionais possuem acesso e podem alterar dados cadastrais de alunos; Impressão de documento físico sem que haja necessidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Envio de documentos por meio digital [Organizacional]; Revisar as permissões de acesso para que os dados não sejam acidentalmente alterados por outros regionais [Segurança da Informação]; Impressão somente de documentos necessários. [Organizacional]	1	1	1

CEPs 02 - Gerenciar avaliação de alunos	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
COORD EAD 06 - Acompanhar Processos de Inscrição e Matrícula dos Ciclos Ativos	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
COORD EAD 04 - Viabilizar a criação do código validador dos alunos dos cursos tec	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

GETI 02 - Atender chamados de TI	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Compartilhamento de dados do titular sem que este tenha conhecimento; Exclusão acidental dos dados ou problemas nos meios de armazenamento	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Informar os titulares da possibilidade de compartilhamento dos dados com este operador [Jurídico]; Revisar Política de Backup [Segurança da Informação]	1	3	3
GETI 01 - Criar acesso aos sistemas	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
COORD EAD 01 - Coletar dados para matrícula de alunos em cursos técnicos EAD - PSG	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

BOP 01 - Receber currículo para cadastro no BOP	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	2	2
DR 05 - Divulgar documentos norteadores na intranet.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
BOP 03 - Realizar controle de requerimento	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

Central de atendimento 05 - Emitir declarações para aluno	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	2	2
CIC 04 - Realizar empréstimos e devoluções de livros	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]	1	1	1
GCELC 01 - Realizar Processo Licitatórios - Fase Interna	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1

CEP CM e GT 01 - Contratar serviços	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
Controladoria 04 - Realizar auditoria interna	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	3	3
Ouvidoria 01 - Gerenciar o canal de ouvidoria	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Informar os titulares da possibilidade de compartilhamento dos dados com este operador [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

GFI 08 - Monitorar inadimplências.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Impressão de documento físico sem que haja necessidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Impressão somente de documentos necessários. [Organizacional]	1	2	2
Controladoria 01 - Realizar auditoria do conselho fiscal	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	2	2
COORD EAD 03 - Matricular alunos na modalidade FIC	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina	2	3	6

		ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]			
CEPs 03 - Realizar acompanhamento de matrículas	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Exclusão acidental dos dados ou problemas nos meios de armazenamento	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar Política de Backup [Segurança da Informação]	1	1	1
CEP GT 02 - Realizar matrícula de alunos	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

Gerência comercial 02 - Estabelecer parceria com convênio	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
CEP GT 03 - Receber equipamentos e utensílios	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Uso de formulário e documentos em papel ; Envio de documentos em via física	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Envio de documentos por meio digital [Organizacional]	1	1	1
GFI 01 - Realizar pagamento das notas fiscais de serviço - PF.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Envio de documentos em via física	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Envio de documentos por meio digital [Organizacional]	1	1	1

SETES 03 - Reapresentar pagamento de devolução.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
RH 12 - Realizar processamento Férias	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Exclusão acidental dos dados ou problemas nos meios de armazenamento; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Revisar Política de Backup [Segurança da Informação]; Implementar medidas de segurança física e do ambiente [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	2	4

GCELC 02 - Realizar Processo Licitatórios - Fase externa	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
GFI 05 - Realizar pagamento de devolução.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Demais regionais possuem acesso e podem alterar dados cadastrais de alunos; Envio de documentos em via física	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Revisar as permissões de acesso para que os dados não sejam acidentalmente alterados por outros regionais [Segurança da Informação]; Envio de documentos por meio digital [Organizacional]	1	1	1

GPC 03 - Enviar dados de alunos para o DN para realização de pesquisa	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
CEPs 04 - Receber atestado e declarações de alunos	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Envio de Dados por Whatsapp	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Não receber atestados/declarações médicas por whatsapp [Segurança da Informação]	1	2	2

SETES 01 - Realizar fechamento de caixa.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
Controladoria 02 - Atender fiscalização contínua do TCU	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

DR 01 - Colher dados para a auditoria interna.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Envio de documentos em via física; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Envio de documentos por meio digital [Organizacional]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	1	2
Secretaria 05 - Enviar dados de aluno ao Bem legal	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Envio de documentos em via física	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Envio de documentos por meio digital [Organizacional]	1	1	1

GEP 01 - Capacitar colaboradores	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
BOP 05 - Elaborar relatórios gerenciais	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
Secretaria 03 - Cadastrar turmas e alunos no SISTEC	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

GETI 03 - Criar login de fornecedores na rede virtual	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
CEP CM, Arapiraca E UPS 01 - Realizar acompanhamento pedagógico	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Impressão de documento físico sem que haja necessidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Acompanhar situação por meio digital [Organizacional]	1	1	1
COORD EAD 08 - Receber relatório de resultado de seleção de estágio	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	1	1	1

COORD EAD 10 - Acompanhar emissão de diplomas dos cursos técnicos	Vazamento por intermédio do funcionário; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
Central de atendimento 01 - Atender solicitação de alunos	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
SETES 02 - Agendar pagamentos de boletos e depósitos	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1

BOP 04 - Atender solicitações de empresas de recrutamento	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	1	2
Ouvidoria 02 - Gerenciar o Fale Conosco	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Informar os titulares da possibilidade de compartilhamento dos dados com este operador [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	1	2
Secretaria 07 - Elaborar ementário escolar	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	1	2

CEPs 06 - Alocar instrutores e coordenadores nas turmas	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Exclusão acidental dos dados ou problemas nos meios de armazenamento	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar Política de Backup [Segurança da Informação]	1	1	1
GCELC 05 - Realizar a gestão contratual.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
CIC 03 - Cadastrar alunos na plataforma digital	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
Secretaria 02 - Realizar cronograma de visita aos postos avançados e Arapiraca	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo	1	1	1

		para o descarte de dados após o fim da finalidade de tratamento [Organizacional]			
RH 09 - Treinar e Desenvolver colaborador	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	1	2
Call center 01 - Atender solicitação de reserva de vagas e demandas	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após	1	2	2

		o fim da finalidade de tratamento [Organizacional]			
RH 11 - Elaborar folha de Pagamento	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Uso de formulário e documentos em papel ; Exclusão acidental dos dados ou problemas nos meios de armazenamento; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Digitalização do processo [Segurança da Informação]; Revisar Política de Backup [Segurança da Informação]; Implementar medidas de segurança física e do ambiente [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	2	4

UPS 02 - Realizar parcerias através de convênios	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	1	2
GSAI 01 - Realizar o controle de acesso às unidades	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Acesso indevido às informações do servidor	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]	1	1	1
Gerência comercial 03 - Visitar e prospectar clientes	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1

DR 03 - Encaminhar demandas dos planos diretores.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
CEP GT 06 - Realizar acompanhamento pedagógico	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
CEPs 09 - Realizar planejamento de execução do curso	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do	2	2	4

		sistema após o fim da finalidade de tratamento [Segurança da Informação]			
CEP CM, Arapiraca e GT 01 - Elaborar termo de compromisso para estágio	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Recebimento de documentos físicos	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]; Recebimento de documentos por meio digital [Organizacional]	1	1	1
DR 02 - Responder notificação judicial.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	2	2

CEP GT 01 - Comunicar início de turma para instrutores ou convidados	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	2	4
GFI 03 - Realizar pagamentos - Diárias	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
GMAC 01 - Produzir materiais para divulgação.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Envio de Dados por Whatsapp; Uso da imagem do titular sem consentimento; Não obtenção de consentimento do titular dos dados; Não há procedimento estabelecido para o	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Solicitar consentimento do titular dos dados [Jurídico]; Informar os titulares da possibilidade de compartilhamento dos dados com este operador [Jurídico]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da	1	3	3

	descarte dos dados do sistema após o atingimento da finalidade	finalidade de tratamento [Segurança da Informação]			
RH 08 - Gerenciar benefícios	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Uso de formulário e documentos em papel ; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Utilização de Formulários Digitais [Organizacional]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	2	4

RH 01 - Recrutar novos colaboradores	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Exclusão acidental dos dados ou problemas nos meios de armazenamento; Não obtenção de consentimento do titular dos dados	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Revisar Política de Backup [Segurança da Informação]; Implementar medidas de segurança física e do ambiente [Segurança da Informação]; Solicitar consentimento do titular dos dados [Jurídico]	2	2	4
GCELC 03 - Realizar requisição de pedido de compra	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	2	2

COORD EAD 11 - Acompanhar situação dos alunos dos cursos téc com documentação pendente	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
GEP 02 - Emitir planilha de dados dos alunos	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
Central de atendimento 04 - Realizar matrícula in company ou convênio	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

COORD EAD 02 - Fornecer relatórios dos cursos realizados pelo EAD	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
RH 04 - Cadastrar colaborador	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Exclusão acidental dos dados ou problemas nos meios de armazenamento; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar Política de Backup [Segurança da Informação]; Implementar medidas de segurança física e do ambiente [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	2	4

GFI 06 - Recolher imposto de renda de aluguéis.	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Envio de documentos em via física; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Envio de documentos por meio digital [Organizacional]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	1	2
Secretaria 06 - Coletar dados para o censo escolar e sistema censo básico	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4

GCELC 04 - Elaborar contrato ou ARP	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Circulação externa de documentos; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Envio de documentos por meio digital [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
CEP GT 04 - Enviar dados de seguro	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1

RH 03 - Encaminhar e marcar exame admissional do colaborador	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Exclusão acidental dos dados ou problemas nos meios de armazenamento; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Revisar Política de Backup [Segurança da Informação]; Implementar medidas de segurança física e do ambiente [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	3	6
RH 07 - Gerenciar os exames de saúde ocupacional	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	3	6

CIC 02 - Realizar backup	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Exclusão acidental dos dados ou problemas nos meios de armazenamento	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Revisar Política de Backup [Segurança da Informação]	1	2	2
UPS 01 - Realizar matrícula dos alunos	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	2	2	4
Call center 02 - Atender solicitações	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Envio de Dados por Whatsapp	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Não utilizar o celular pessoal do colaborador no processo [Organizacional]; Não	2	2	4

		enviar dados pessoais dos alunos via whatsapp [Segurança da Informação]			
GECOR 03 - Enviar declarações para órgãos fiscais	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
GSAI 03 - Entregar correspondência	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1

Secretaria 08 - Emitir certidões	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]	1	1	1
RH 10 - Registrar e realizar manutenção do ponto	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Uso de formulário e documentos em papel ; Exclusão acidental dos dados ou problemas nos meios de armazenamento; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Envio de documentos por meio digital [Organizacional]; Revisar Política de Backup [Segurança da Informação]; Implementar medidas de segurança física e do ambiente [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	3	6
Central de atendimento 03 - Abrir e fechar caixa	Vazamento por intermédio do funcionário; Acesso indevido às informações físicas; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Implementar rotina ou processo	2	2	4

		para o descarte de dados após o fim da finalidade de tratamento [Organizacional]			
CEPs 05 - Aprovar informações para encerramento de produção mensal	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados do sistema após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento [Segurança da Informação]	2	2	4
DR 04 - Compartilhar arquivos via Google Drive ou E-mail.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Uso da imagem do titular sem consentimento	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Solicitar consentimento do titular dos dados [Jurídico]	2	1	2
GETI 05 - Gerar relatórios para outros setores	Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Informar os titulares da possibilidade de compartilhamento dos dados com este operador [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Revisar as permissões de	2	2	4

		acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]			
CEPs 10 - Gerenciar frequência de aluno	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade; Envio de Dados por Whatsapp	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]; Não enviar dados pessoais dos alunos via whatsapp [Segurança da Informação]	1	1	1
GFI 02 - Realizar pagamentos - Educação corporativa.	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte	2	1	2

		de dados após o fim da finalidade de tratamento [Organizacional]			
GETI 04 - Realizar backup	Vazamento por intermédio do funcionário; Acesso indevido às informações do servidor; Exclusão acidental dos dados ou problemas nos meios de armazenamento; A restauração de um backup pode retornar dados excluídos das bases de dados ou desatualizadas (relacionado à excução de direitos dos titulares)	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Revisar Política de Backup [Segurança da Informação]; Garantir que todos os logs de alteração das bases sejam replicadas aos backups quando da sua reutilização [Segurança da Informação]	1	3	3
GECOR 02 - Elaborar o balanço anual	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações físicas; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Controlar acesso ao local de armazenamento de documentos físicos [Organizacional]; Revisar as permissões de acesso [Segurança da Informação]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1

Controladoria 03 - Enviar dados estratégicos para o portal da transparência	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1
Controladoria 05 - Elaborar relatórios de gestão	Acesso indevido às informações dos sistemas de informação ou e-mails; Vazamento por intermédio do funcionário; Vazamento de dados no operador; Acesso indevido às informações do servidor; Não há procedimento estabelecido para o descarte dos dados após o atingimento da finalidade	Capacitar os colaboradores em segurança da informação e privacidade [Organizacional]; Revisar a política de atualização de senhas [Segurança da Informação]; Revisar as permissões de acesso [Segurança da Informação]; Revisar termo de sigilo e coletar assinatura do funcionário [Jurídico]; Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais [Jurídico]; Implementar rotina ou processo para o descarte de dados após o fim da finalidade de tratamento [Organizacional]	1	1	1

5 - Tratamento dos riscos

O tratamento dos riscos foi totalmente elaborado em forma de planos de ações, deixando claro como será a sua execução. O responsável e o prazo de conclusão de cada plano deve ser definido pelo SENAC AL.

Controle	Classificação	Processos	Responsável	Quando
Acompanhar situação por meio digital	Organizacional	CEP CM, Arapiraca E UPS 01 - Realizar acompanhamento pedagógico	SENAC-AL	
Capacitar os colaboradores em segurança da informação e privacidade	Organizacional	Todos os processos	ADX	
Controlar acesso ao local de armazenamento de documentos físicos	Organizacional	GFI 04 - Pagar NF ou fatura de pessoa jurídica. ; CEP GT E UPS 01 - Gerenciar documentos enviados ao RH; RH 13 - Demitir colaborador; CEPs 01 - Elaborar folha de pagamento; COORD EAD 07 - Acompanhar prática profissional do programa de aprendizagem; GFI 09 - Realizar fechamento de movimentação financeira; RH 05 - Integrar colaboradores; Secretaria 04 - Emitir diploma, certificados e histórico escolar dos alunos ; GEP 03 - Participar das competições SENAC; BOP 02 - Realizar matrícula por convênio social; CEP Arapiraca e Central 01 - Realizar a matrícula de alunos; CIC 01 - Cadastrar alunos e colaboradores na biblioteca; RH 02 - Admitir colaboradores; Gerência comercial 01 - Elaborar proposta ou projeto comercial; Secretaria 01 - Gerenciar o arquivo físico ; GECOR	SENAC-AL	

		01 - Elaborar o balancete; CEPs 07 - Enviar dados de carga horária de instrutores para pagamento; Central de atendimento 02 - Realizar matrícula de alunos via web; CEP GT 05 - Realizar avaliações institucionais; RH 06 - Avaliar desempenho do colaborador ; GFI 07 - Atender solicitações de alunos.; CEPs 02 - Gerenciar avaliação de alunos; DR 05 - Divulgar documentos norteadores na intranet.; Central de atendimento 05 - Emitir declarações para aluno; GCELC 01 - Realizar Processo Licitatórios - Fase Interna; GFI 08 - Monitorar inadimplências.; COORD EAD 03 - Matricular alunos na modalidade FIC; CEP GT 02 - Realizar matrícula de alunos; Gerência comercial 02 - Estabelecer parceria com convênio ; CEP GT 03 - Receber equipamentos e utensílios; SETES 03 - Reapresentar pagamento de devolução.; RH 12 - Realizar processamento Férias; GCELC 02 - Realizar Processo Licitatórios - Fase externa; GFI 05 - Realizar pagamento de devolução.; CEPs 04 - Receber atestado e declarações de alunos; SETES 01 - Realizar fechamento de caixa.; DR 01 - Colher dados para a auditoria interna.; Secretaria 05 - Enviar dados de aluno ao Bem legal; GEP 01 - Capacitar colaboradores ; Central de atendimento 01 - Atender solicitação de alunos; SETES 02 - Agendar pagamentos de boletos e depósitos; Secretaria 07 - Elaborar ementário escolar; Secretaria 02 - Realizar cronograma de visita aos postos avançados e Arapiraca ; RH 09 - Treinar e Desenvolver colaborador; Call center 01 - Atender solicitação de reserva de vagas e demandas; RH 11 - Elaborar folha de Pagamento; UPS 02 - Realizar parcerias através de convênios; GSAI 01 - Realizar o controle de acesso às unidades; Gerência comercial 03 - Visitar e prospectar clientes; DR 03 - Encaminhar demandas dos planos diretores.; CEP GT 06 - Realizar acompanhamento pedagógico; CEP CM, Arapiraca e GT 01 - Elaborar termo de compromisso para estágio; DR 02 - Responder notificação judicial.; GFI 03 - Realizar pagamentos - Diárias; RH 08 - Gerenciar benefícios; RH 01 - Recrutar novos colaboradores; GCELC 03 - Realizar requisição de pedido de compra; GFI 06 - Recolher imposto de renda de aluguéis.; GCELC 04 - Elaborar contrato ou ARP; RH 03 - Encaminhar e marcar exame admissional do colaborador ; RH 07 - Gerenciar os exames de saúde ocupacional ; UPS 01 - Realizar matrícula dos alunos; GECOR 03 - Enviar declarações para órgãos fiscais; GSAI 03 - Entregar correspondência; Secretaria 08 - Emitir certidões; RH 10 - Registrar e realizar manutenção do ponto; Central de atendimento 03 - Abrir e fechar caixa; CEPs 10 - Gerenciar frequência de aluno; GFI 02 - Realizar pagamentos - Educação corporativa.; GECOR 02 - Elaborar o balanço anual		

Digitalização do processo	Segurança da Informação	GFI 09 - Realizar fechamento de movimentação financeira; RH 11 - Elaborar folha de Pagamento	SENAC-AL	
Digitalização dos documentos evitando envio físico dos mesmos	Organizacional	RH 13 - Demitir colaborador	SENAC-AL	
Envio de documentos por meio digital	Organizacional	CEP GT E UPS 01 - Gerenciar documentos enviados ao RH; GFI 07 - Atender solicitações de alunos.; CEP GT 03 - Receber equipamentos e utensílios; GFI 01 - Realizar pagamento das notas fiscais de serviço - PF.; GFI 05 - Realizar pagamento de devolução.; DR 01 - Colher dados para a auditoria interna.; Secretaria 05 - Enviar dados de aluno ao Bem legal; GFI 06 - Recolher imposto de renda de aluguéis.; GCELC 04 - Elaborar contrato ou ARP; RH 10 - Registrar e realizar manutenção do ponto	SENAC-AL	
Garantir que todos os logs de alteração das bases sejam replicadas aos backups quando da sua reutilização	Segurança da Informação	GETI 04 - Realizar backup	SENAC-AL	
Implementar medidas de segurança física no ambiente	Segurança da Informação	RH 13 - Demitir colaborador; RH 05 - Integrar colaboradores; RH 02 - Admitir colaboradores; RH 06 - Avaliar desempenho do colaborador ; RH 12 - Realizar processamento Férias; RH 11 - Elaborar folha de Pagamento; RH 01 - Recrutar novos colaboradores; RH 04 - Cadastrar colaborador ; RH 03 - Encaminhar e marcar exame admissional do colaborador ; RH 10 - Registrar e realizar manutenção do ponto	SENAC-AL	
Implementar rotina ou processo para o descarte de dados do sistema após o fim da finalidade de tratamento	Segurança da Informação	RH 13 - Demitir colaborador; COORD EAD 07 - Acompanhar prática profissional do programa de aprendizagem; RH 05 - Integrar colaboradores; GFI 10 - Emitir notas fiscais de serviços.; RH 02 - Admitir colaboradores; RH 06 - Avaliar desempenho do colaborador ; RH 12 - Realizar processamento Férias; DR 01 - Colher dados para a auditoria interna.; COORD EAD 08 - Receber relatório de resultado de seleção de estágio; RH 09 - Treinar e Desenvolver colaborador; RH 11 - Elaborar folha de Pagamento; CEPs 09 - Realizar planejamento de execução do curso; CEP CM, Arapiraca e GT 01 - Elaborar termo de compromisso para estágio; CEP GT 01 -Comunicar início de turma para instrutores ou convidados; GMAC 01 - Produzir materiais para divulgação.; RH 08 - Gerenciar benefícios; RH 04 - Cadastrar colaborador ; GFI 06 - Recolher imposto de renda de aluguéis.; RH 03 -	SENAC-AL	

		Encaminhar e marcar exame admissional do colaborador ; RH 10 - Registrar e realizar manutenção do ponto; CEPs 05 - Aprovar informações para encerramento de produção mensal		
Impressão somente de documentos necessários.	Organizacional	GFI 07 - Atender solicitações de alunos.; GFI 08 - Monitorar inadimplências.	SENAC-AL	
Informar os titulares da possibilidade de compartilhamento dos dados com este operador	Jurídico	CEPs 08 - Gerenciar grupo da turma em redes sociais e ambiente virtual; GETI 02 - Atender chamados de TI; Ouvidoria 01 - Gerenciar o canal de ouvidoria; Ouvidoria 02 - Gerenciar o Fale Conosco; GMAC 01 - Produzir materiais para divulgação.; GETI 05 - Gerar relatórios para outros setores	SENAC-AL	
Não enviar dados pessoais dos alunos via whatsapp	Segurança da Informação	CEPs 08 - Gerenciar grupo da turma em redes sociais e ambiente virtual; COORD EAD 07 - Acompanhar prática profissional do programa de aprendizagem; Call center 02 - Atender solicitações; CEPs 10 - Gerenciar frequência de aluno	SENAC-AL	
Não receber atestados/declarações médicas por whatsapp	Segurança da Informação	CEPs 04 - Receber atestado e declarações de alunos	SENAC-AL	
Não utilizar o celular pessoal do colaborador no processo	Organizacional	CEPs 08 - Gerenciar grupo da turma em redes sociais e ambiente virtual; Call center 02 - Atender solicitações	SENAC-AL	
Recebimento de documentos por meio digital	Organizacional	GFI 04 - Pagar NF ou fatura de pessoa jurídica; CEP CM, Arapiraca e GT 01 - Elaborar termo de compromisso para estágio	SENAC-AL	
Revisar a política de atualização de senhas	Segurança da Informação	Todos os processos	SENAC-AL	
Revisar as permissões de acesso	Segurança da Informação	Todos os processos	SENAC-AL	

Revisar as permissões de acesso para que os dados não sejam acidentalmente alterados por outros regionais	Segurança da Informação	GFI 07 - Atender solicitações de alunos.; GFI 05 - Realizar pagamento de devolução.	SENAC-AL	
Revisar Política de Backup	Segurança da Informação	RH 13 - Demitir colaborador; RH 05 - Integrar colaboradores; RH 02 - Admitir colaboradores; RH 06 - Avaliar desempenho do colaborador ; GETI 02 - Atender chamados de TI; CEPs 03 - Realizar acompanhamento de matrículas; RH 12 - Realizar processamento Férias; CEPs 06 - Alocar instrutores e coordenadores nas turmas; RH 11 - Elaborar folha de Pagamento; RH 01 - Recrutar novos colaboradores; RH 04 - Cadastrar colaborador ; RH 03 - Encaminhar e marcar exame admissional do colaborador ; CIC 02 - Realizar backup; RH 10 - Registrar e realizar manutenção do ponto; GETI 04 - Realizar backup	ADX	
Revisar termo de sigilo e coletar assinatura do funcionário	Jurídico	Todos os processos	SENAC-AL	

Revisão do contrato ou notificação dos operadores referente ao tratamento de dados pessoais	Jurídico	GFI 04 - Pagar NF ou fatura de pessoa jurídica. ; GPC 01 - Realizar o cadastro no sistema Qualiex; RH 13 - Demitir colaborador; CEPs 01 - Elaborar folha de pagamento; COORD EAD 07 - Acompanhar prática profissional do programa de aprendizagem; GSAI 02 - Realizar o controle de contratos; GFI 09 - Realizar fechamento de movimentação financeira; Secretaria 04 - Emitir diploma, certificados e histórico escolar dos alunos ; GFI 10 - Emitir notas fiscais de serviços.; Call center 03 - Captar leads; GEP 03 - Participar das competições SENAC; CEP Arapiraca e Central 01 - Realizar a matrícula de alunos; CIC 01 - Cadastrar alunos e colaboradores na biblioteca; Gerência comercial 01 - Elaborar proposta ou projeto comercial; GECOR 01 - Elaborar o balancete; CEPs 07 - Enviar dados de carga horária de instrutores para pagamento; GPC 02 - Receber a produção institucional (GEP); COORD EAD 05 - Responder demandas do Fale Conosco e ouvidoria; Central de atendimento 02 - Realizar matrícula de alunos via web; COORD EAD 09 - Acompanhar o processo de matrícula dos alunos PROUNI; CEP GT 05 - Realizar avaliações institucionais; GFI 07 - Atender solicitações de alunos.; CEPs 02 - Gerenciar avaliação de alunos; COORD EAD 06 - Acompanhar Processos de Inscrição e Matrícula dos Ciclos Ativos; COORD EAD 04 - Viabilizar a criação do código validador dos alunos dos cursos tec; GETI 02 - Atender chamados de TI; GETI 01 - Criar acesso aos sistemas; COORD EAD 01 - Coletar dados para matrícula de alunos em cursos técnicos EAD - PSG; BOP 01 - Receber currículo para cadastro no BOP; DR 05 - Divulgar documentos norteadores na intranet.; Central de atendimento 05 - Emitir declarações para aluno; CIC 04 - Realizar empréstimos e devoluções de livros; GCELC 01 - Realizar Processo Licitatórios - Fase Interna; CEP CM e GT 01 - Contratar serviços; Controladoria 04 - Realizar auditoria interna; Ouvidoria 01 - Gerenciar o canal de ouvidoria; GFI 08 - Monitorar inadimplências.; Controladoria 01 - Realizar auditoria do conselho fiscal; COORD EAD 03 - Matricular alunos na modalidade FIC; CEPs 03 - Realizar acompanhamento de matrículas; CEP GT 02 - Realizar matrícula de alunos; Gerência comercial 02 - Estabelecer parceria com convênio ; GFI 01 - Realizar pagamento das notas fiscais de serviço - PF.; SETES 03 - Reapresentar pagamento de devolução.; RH 12 - Realizar processamento Férias; GCELC 02 - Realizar Processo Licitatórios - Fase externa; GFI 05 - Realizar pagamento de devolução.; GPC 03 - Enviar dados de alunos para o DN para realização de pesquisa; CEPs 04 - Receber atestado e declarações de alunos; SETES 01 - Realizar fechamento de caixa.; Controladoria 02 - Atender fiscalização contínua do TCU; DR 01 - Colher dados para a auditoria interna.;	ADX	

		Secretaria 05 - Enviar dados de aluno ao Bem legal; GEP 01 - Capacitar colaboradores ; BOP 05 - Elaborar relatórios gerenciais; Secretaria 03 - Cadastrar turmas e alunos no SISTEC; GETI 03 - Criar login de fornecedores na rede virtual; CEP CM, Arapiraca E UPS 01 - Realizar acompanhamento pedagógico; COORD EAD 08 - Receber relatório de resultado de seleção de estágio; COORD EAD 10 - Acompanhar emissão de diplomas dos cursos técnicos; SETES 02 - Agendar pagamentos de boletos e depósitos; BOP 04 - Atender solicitações de empresas de recrutamento; Ouvidoria 02 - Gerenciar o Fale Conosco; CEPs 06 - Alocar instrutores e coordenadores nas turmas; GCELC 05 - Realizar a gestão contratual.; CIC 03 - Cadastrar alunos na plataforma digital; RH 09 - Treinar e Desenvolver colaborador; Call center 01 - Atender solicitação de reserva de vagas e demandas; RH 11 - Elaborar folha de Pagamento; UPS 02 - Realizar parcerias através de convênios; Gerência comercial 03 - Visitar e prospectar clientes; DR 03 - Encaminhar demandas dos planos diretores.; CEP GT 06 - Realizar acompanhamento pedagógico; CEPs 09 - Realizar planejamento de execução do curso; DR 02 - Responder notificação judicial.; CEP GT 01 -Comunicar início de turma para instrutores ou convidados; GFI 03 - Realizar pagamentos - Diárias; RH 08 - Gerenciar benefícios; GCELC 03 - Realizar requisição de pedido de compra; COORD EAD 11 - Acompanhar situação dos alunos dos cursos téc com documentação pendente; GEP 02 - Emitir planilha de dados dos alunos ; Central de atendimento 04 - Realizar matrícula in company ou convênio; COORD EAD 02 - Fornecer relatórios dos cursos realizados pelo EAD; RH 04 - Cadastrar colaborador ; GFI 06 - Recolher imposto de renda de aluguéis.; Secretaria 06 - Coletar dados para o censo escolar e sistema censo básico; GCELC 04 - Elaborar contrato ou ARP; CEP GT 04 - Enviar dados de seguro; RH 03 - Encaminhar e marcar exame admissional do colaborador ; RH 07 - Gerenciar os exames de saúde ocupacional ; CIC 02 - Realizar backup; UPS 01 - Realizar matrícula dos alunos; Call center 02 - Atender solicitações; GECOR 03 - Enviar declarações para órgãos fiscais; RH 10 - Registrar e realizar manutenção do ponto; CEPs 05 - Aprovar informações para encerramento de produção mensal; DR 04 - Compartilhar arquivos via Google Drive ou E-mail.; GETI 05 - Gerar relatórios para outros setores; CEPs 10 - Gerenciar frequência de aluno; GFI 02 - Realizar pagamentos - Educação corporativa.; GECOR 02 - Elaborar o balanço anual; Controladoria 05 - Elaborar relatórios de gestão		

Solicitar consentimento do titular dos dados	Jurídico	GMAC 01 - Produzir materiais para divulgação.; RH 01 - Recrutar novos colaboradores; DR 04 - Compartilhar arquivos via Google Drive ou E-mail.	SENAC-AL	
Utilização de Formulários Digitais	Organizacional	RH 13 - Demitir colaborador; RH 08 - Gerenciar benefícios	SENAC-AL	
Disponibilizar o contato do DPO para os titulares no site da empresa	Jurídico	Todos os processos	SENAC-AL	
Adicionar a função do DPO no organograma	Jurídico	Todos os processos	ADX	
Criar a ficha de descrição do cargo de DPO	Jurídico	Todos os processos	ADX	
Capacitar o DPO	Segurança da Informação	Todos os processos	ADX	
Elaborar o processo de análise de impacto à privacidade para novos projetos	Segurança da Informação	Todos os processos	ADX	
Elaborar o processo de gestão de incidentes de segurança e privacidade	Segurança da Informação	Todos os processos	ADX	
Implementar os processos para atendimento dos direitos dos titulares segundo a LGPD	Jurídico	Todos os processos	ADX	
Institucionalizar o comitê de gestão de segurança e privacidade	Jurídico	Todos os processos	SENAC-AL	

Criar e-book sobre boas práticas em proteção de dados para enviar a todos os fornecedores	Segurança da Informação	Todos os processos	ADX	
Criar template para avaliação de legitimo interesse	Jurídico	Todos os processos	ADX	
Criar vídeo aulas sobre proteção de dados para capacitação dos novos colaboradores	Segurança da Informação	Todos os processos	ADX	
Excluir todos os dados que alcançaram o seu período de retenção	Segurança da Informação	Todos os processos	SENAC-AL	
Implantar ferramenta para registro centralizado dos logs dos servidores e ativos de rede	Segurança da Informação	Todos os processos	SENAC-AL	
Ativar processo de auditoria no Active Directory	Segurança da Informação	Todos os processos	SENAC-AL	
Ativar processo de auditoria nas pastas críticas do servidor de arquivo	Segurança da Informação	Todos os processos	SENAC-AL	
Centralizar os documentos existentes nas máquinas dos colaboradores no servidor de arquivos local ou no Drive na nuvem	Segurança da Informação	Todos os processos	SENAC-AL	

Ativar recursos de criptografia nos computadores móveis	Segurança da Informação	Todos os processos	SENAC-AL	
Definir processo de auditoria do SGPD	Segurança da Informação	Todos os processos	ADX	
Criar o repositório de documentos do SGPD	Segurança da Informação	Todos os processos	ADX	
Validar periodicamente os membros dos grupos de administradores de empresa do AD	Segurança da Informação	Todos os processos	SENAC-AL	
Ajustar o código de conduta com requisitos da LGPD	Segurança da Informação	Todos os processos	ADX	
Fazer notificações especiais aos fornecedores que tratam dados pessoais em nome do SENAC-AL	Jurídico	Todos os processos	ADX	
Implantar processo de auditoria de segurança e proteção de dados	Segurança da Informação	Todos os processos	ADX	
Corrigir as vulnerabilidades de segurança detectadas nas redes internas e site	Segurança da Informação	Todos os processos	SENAC-AL	
Reduzir a quantidade de papéis nas mesas implantando a política de mesa limpa	Segurança da Informação	Todos os processos	SENAC-AL	

Concluir implantação do serviço de WSUS para atualização automatizada das correções de segurança nos computadores da rede	Segurança da Informação	Todos os processos	SENAC-AL	
Adicionar política de privacidade e consentimento no formulário de cadastro de uso do Wi-fi	Jurídico	Todos os processos	SENAC-AL	
Adicionar política de privacidade e consentimento no formulário de coleta de currículos do site	Jurídico	Todos os processos	SENAC-AL	
Aumentar o nível de segurança da política de senhas do domínio	Segurança da Informação	Todos os processos	SENAC-AL	
Elaborar e implantar a política de classificação das informações	Segurança da Informação	Todos os processos	ADX	
Elaborar política de recuperação contra desastres	Segurança da Informação	Todos os processos	ADX	
Ajustar a política de segurança da informação	Segurança da Informação	Todos os processos	ADX	
Elaborar acordo de confidencialidade para colaboradores e prestadores de serviço	Segurança da Informação	Todos os processos	ADX	

Remover a opção "Senha nunca expira" da conta de todos os usuários do domínio	Segurança da Informação	Todos os processos	SENAC-AL	
Implantar política de mesa limpa para reduzir a exposição de dados pessoais em papeis impressos	Segurança da Informação	Todos os processos	SENAC-AL	
Elaborar modelo de Relatório de Impacto à Proteção de Dados	Segurança da Informação	Todos os processos	ADX	
Implementar correções descritas no RIPD do sistema analisado.	Segurança da Informação	Todos os processos	SENAC-AL	
Elaborar política de privacidade externa	Jurídico	Todos os processos	ADX	
Elaborar política de proteção de dados	Jurídico	Todos os processos	ADX	
Construir o portal da privacidade	Jurídico	Todos os processos	ADX	
Criar política para contas de serviço do AD	Segurança da Informação	Todos os processos	SENAC-AL	
Implantar solução para monitoramento dos ativos de rede e serviços críticos.	Segurança da Informação	Todos os processos	SENAC-AL	

Atualizar os sistemas operacionais descontinuados	Segurança da Informação	Todos os processos	SENAC-AL	
Atualizar a versão do sistema gerenciador do banco de dados	Segurança da Informação	Todos os processos	SENAC-AL	
Elaborar programa de governança em privacidade	Segurança da Informação	Todos os processos	ADX	