Práticas de Privacidade e Proteção de Dados

Cagece

CEARÁ
GOVERNO DO ESTADO
SECRETARIA DAS CIDADES

Felipe Rodrigues de Oliveira
Coordenador de Segurança da Informação
Analista de Privacidade e Proteção de Dados Pessoais
felipe.rodrigues@cagece.com.br

Lei Nº. 13.709 (Lei Geral de Proteção de Dados – LGPD)

Nossa Cagece

2.219.768
Clientes de Água

Fornecedores

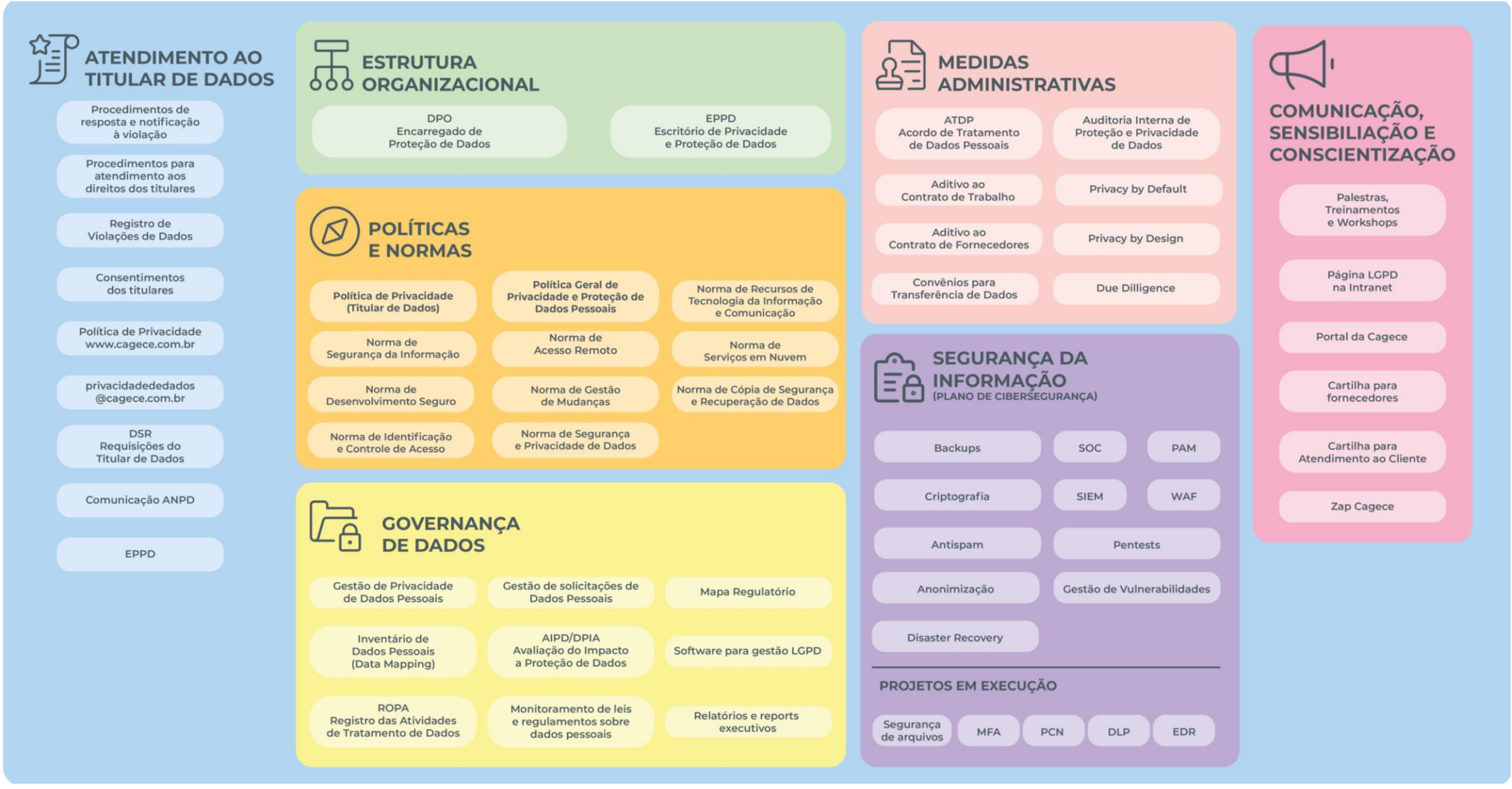
534

Contratos ativos

Colaboradores

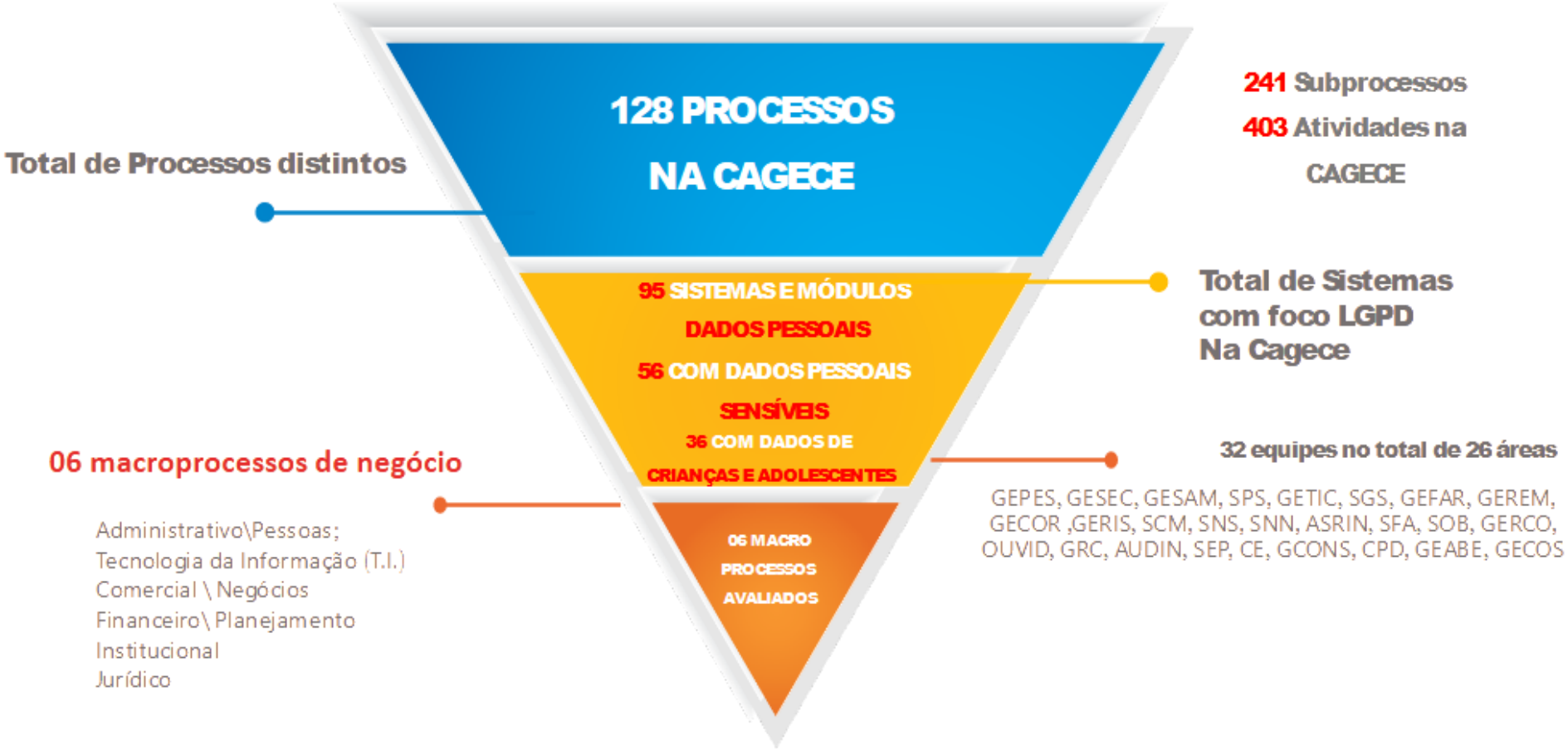
Empregados próprios	1.143
Terceirizados	4.328
Estagiários	266
Jovens Aprendizes	38

Framework LGPD Cagece

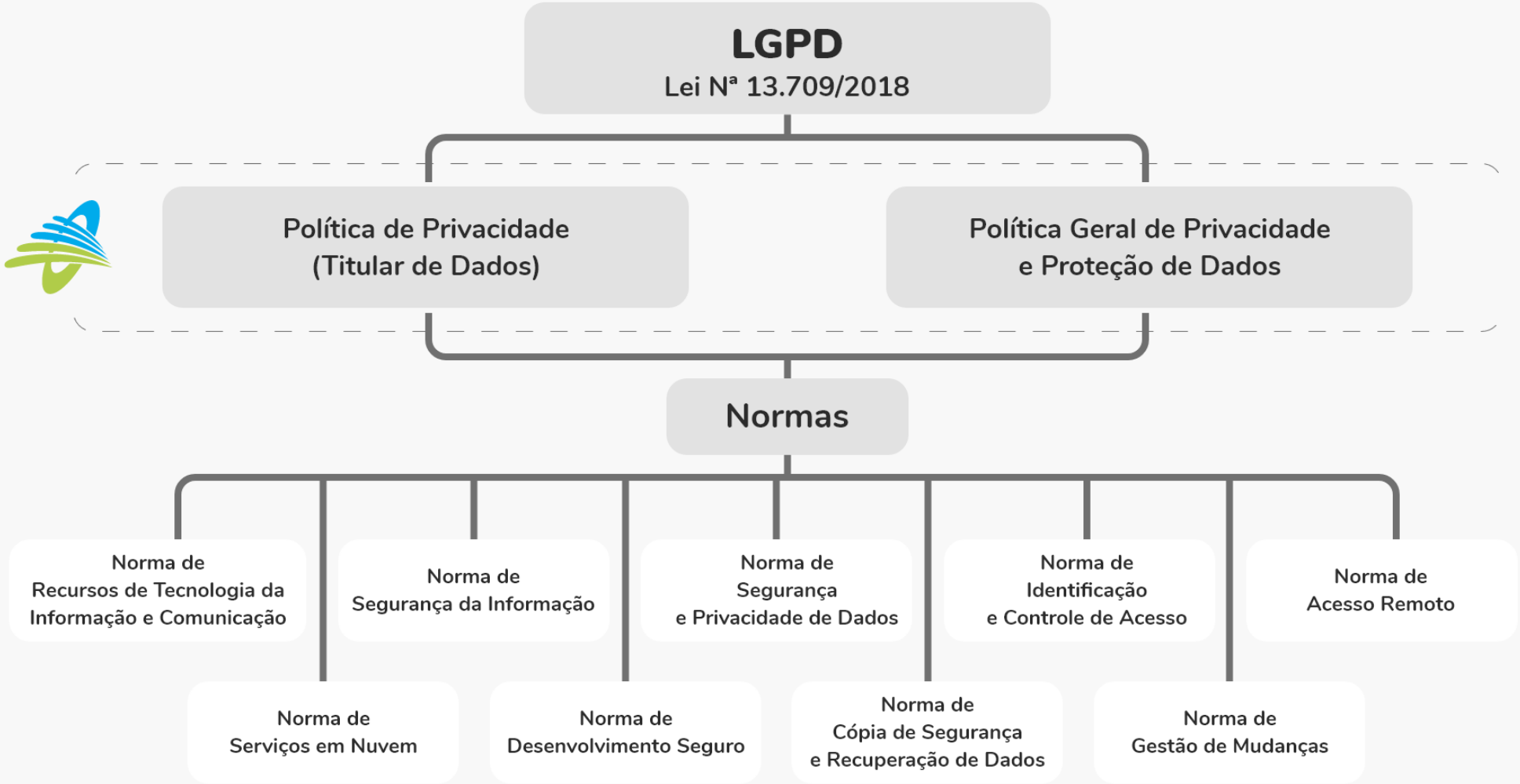


Escritório de Privacidade e Proteção de Dados - EPPD

LGPD na Cagece



Normativos


LGPD
Lei Nª 13.709/2018
Política de Privacidade
(Titular de Dados)
Política Geral de Privacidade
e Proteção de Dados
Normas
Norma de
Recursos de Tecnologia da
Informação e Comunicação
Norma de
Segurança da Informação
Norma de
Segurança
e Privacidade de Dados
Norma de
Identificação
e Controle de Acesso
Norma de
Acesso Remoto
Norma de
Serviços em Nuvem
Norma de
Desenvolvimento Seguro
Norma de
Cópia de Segurança
e Recuperação de Dados
Norma de
Gestão de Mudanças

Privacy by design e privacy by default

4.1.1 Principios de Arquitetura e Engenharia de Sistemas Seguros

4.1.1.1 Todo desenvolvimento de produto ou serviços, devem ser planejados desde a sua concepção com requisitos de privacidade e proteção de dados, devendo ser utilizado os princípios de arquitetura de segurança e privacidade por padrão como "Segurança por design","Defesa em Profundidade", "Segurança por Padrão", "Negar por padrão", " Desconfiar de entrada de aplicações externas", "Segurança na implantação", "Menor Privilégio", dentre outros princípios de segurança e privacidade de dados;

4.1.1.2 Na fase inicial do projeto de desenvolvimento de software, deve ser incluída a equipe de Segurança da informação para discussão, análise e validação de controles de segurança que serão utilizados no software.

4.1.1.3 Os servidores que mantém as aplicações devem ser homologados do ponto de vista de segurança da informação e devem se manter sempre atualizados contra vulnerabilidades conhecidas.

4.1.1.4 Os códigos fonte devem ser armazenados em local seguro, com tecnologias de mercado, com acessos restritos, e proteção contra vazamento de dados.

4.1.1.5 Toda aplicação deverá ser configurada para evitar a listagem de seus diretórios, evitando assim, que um atacante tenha conhecimento da sua estrutura de arquivos e pastas; A aplicação deverá ser configurada e desenvolvida para que não exiba mensagens de erro detalhadas, tais como mensagens de debug. Ao invés disso, o desenvolvedor poderá armazenar ou repassar internamente as mensagens. As mensagens de erro devem conter informações mínimas que ajudem o usuário no problema, mas que não forneçam informações desnecessárias.

4.1.1.6 Deverá ser utilizado sistemas de bancos de dados de mercado, atualizados e suportados pelos respectivos fabricantes.

4.1.1.7 Servidores de teste, homologação ou qualquer outro ambiente devem ser totalmente segregados dos servidores de produção.

4.1.1.8 Deve-se utilizar um controle de versão distribuído, que mantém um repositório completo em cada máquina de desenvolvimento.

4.1.1.9 Deve-se assegurar que as bibliotecas externas sejam gerenciadas(por exemplo, mantendo um inventário de bibliotecas utilizadas e suas versões) e atualizadas regularmente com ciclos de lançamento.

4.1.1.10 Assegurar que o software seja mantido, rastreado e originário de fontes

Av. Dr. Lauro Vieira Chaves, 1030 - Vila União
CEP: 60422-901 • Fortaleza / CE
CNPJ: 07.040.108/0001-57

Cagece

CEARÁ
GOVERNO DO ESTADO
SECRETARIA DAS CIDADES

comprovadas e respeitáveis.

4.1.1.11 Implantar e manter um registro de auditoria de todos os acessos a código-fonte de programa.

4.1.2 Ciclo de Vida do Desenvolvimento de Software Seguro

4.1.2.1 O ciclo de vida de um software refere-se às etapas do processo de software de ponta-a-ponta, desde a concepção, desenvolvimento, operação até a manutenção ou descontinuidade de um software, abrangendo toda a vida do sistema.

4.1.2.2 Na fase de levantamento de requisitos deverá ser mapeado e documentado todos os dados pessoais a serem coletados pelo software a ser desenvolvido.

4.1.2.3 Todos os campos que coletam dados pessoais no sistema devem ser mapeados, e a área de negócio gestora do software deverá informar a finalidade, base legal e tempo de retenção dos dados, devendo essa informação ser armazenada juntamente com a documentação do software.

4.1.2.4 No processo de desenvolvimento de sistemas deve considerar o tempo para implantação dos controles de segurança nos projetos, bem como levar em consideração o tempo para realizações de testes de validações de segurança.

4.1.2.5 O desenvolvedor deverá identificar e informar a Cagece quanto às exceções necessárias para quanto à verificação do sistema de antivírus. (pastas, arquivos e processos).

4.1.3 Direitos de Acessos Privilegiados

4.1.3.1 Os desenvolvedores não devem ter acesso aos servidores do ambiente de produção.

4.1.3.2 Os desenvolvedores não devem ter acesso aos bancos de dados do ambiente de produção.

4.1.3.3 Os desenvolvedores não devem ter acesso de administrador nas máquinas.

4.1.3.4 Deve-se estabelecer regra baseada na premissa "Tudo é proibido, a menos que expressamente permitido" em lugar da regra mais fraca "Tudo é permitido, a menos que expressamente proibido".

4.1.3.5 O desenvolvedor não deve utilizar comentários ou textos nos códigos, com caráter pejorativo, racista, político ou qualquer outro que não seja referente ao código do sistema corporativo.

Plano de Resposta a Incidentes

1 APRESENTAÇÃO

Este documento estabelece o Plano de Resposta a Incidentes alinhado com os requisitos da Lei Geral de Proteção de Dados (LGPD) e Política de Privacidade e Proteção de Dados Pessoais O objetivo principal deste plano é definir os procedimentos e responsabilidades para a detecção, análise, contenção, erradicação, recuperação e pós-incidente de violações de dados pessoais, minimizando seus impactos e garantindo a conformidade legal e regulatória.

Para a Companhia de Água e Esgoto do Ceará (Cagece), uma empresa que presta serviços essenciais e lida com um vasto volume de dados pessoais de seus clientes e colaboradores, a proteção de dados é uma prioridade estratégica. A Cagece coleta e trata informações como CPF, e-mail, número de telefone e geolocalização para a prestação de seus serviços de captação, tratamento e distribuição de água, bem como coleta e tratamento de esgoto sanitário em todo o estado do Ceará.

A natureza desses dados, que incluem informações de identificação pessoal e, em alguns casos, dados financeiros relacionados ao consumo e pagamentos, torna a Cagece um alvo potencial para incidentes de segurança e privacidade. A implementação de um plano robusto é fundamental para a Cagece, não apenas para cumprir as exigências da LGPD, mas também para manter a confiança de seus usuários e a integridade de suas operações.

A empresa já demonstra preocupação com a privacidade, possuindo uma framework de Privacidade e Proteção de Dados, que abrange diversas frentes, incluindo o atendimento ao titular de dados, uma estrutura organizacional dedicada com DPO e EPPD, e um robusto conjunto de políticas e normas. Ele também integra medidas administrativas, segurança da informação e governança de dados, além de focar na comunicação e conscientização para garantir a conformidade e a proteção dos dados pessoais. Este plano se integra a essas iniciativas, fortalecendo a capacidade da Cagece de proteger os dados sob sua responsabilidade.

2 FUNDAMENTAÇÃO LEGAL

2.1 Legislação Federal Nº 13.709, de 14 de agosto de 2018, Lei Geral de Proteção de Dados Pessoais.
2.2 RESOLUÇÃO CD/ANPD Nº 15, de 24 de abril de 2024 - Regulamento de Comunicação de Incidente de Segurança
2.3 Política Geral de Privacidade e Proteção de Dados Pessoais
2.4 Norma de Privacidade e Proteção de Dados Pessoais
2.5 Política de Segurança da Informação – PSI
2.6 Norma de Segurança da Informação

Av. Dr. Lauro Vieira Chaves, 1030 - Vila União
CEP: 60422-901 • Fortaleza / CE
CNPJ: 07.040.108/0001-57

3 DEFINIÇÕES E CONCEITOS

3.1 **ANPD (AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS):** Órgão da administração pública federal responsável por zelar pela proteção de dados pessoais e por fiscalizar e aplicar as sanções em caso de descumprimento da LGPD.
3.2 **CONTROLADOR:** Pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
3.3 **DADO PESSOAL:** Informação relacionada a pessoa natural identificada ou identificável
3.4 **DADO PESSOAL SENSÍVEL**: Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a` saúde ou a` vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural
3.5 **ENCARREGADO DOS DADOS**: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)
3.6 **INCIDENTE DE SEGURANÇA:** Qualquer evento adverso, confirmado ou suspeito, relacionado à segurança dos sistemas de informação ou dos dados, que possa comprometer a confidencialidade, integridade ou disponibilidade das informações.
3.7 **INCIDENTE DE PRIVACIDADE / VIOLAÇÃO DE DADOS PESSOAIS:** Um incidente de segurança que resulte na destruição, perda, alteração, acesso não autorizado, ou na divulgação não autorizada ou acidental de dados pessoais transmitidos, armazenados ou de outra forma tratados.
3.8 **OPERADOR:** Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.
3.9 **TITULAR DE DADOS:** Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.
3.10 **TRATAMENTO:** Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

4 ESCOPO E ABRANGÊNCIA

Este PRIP aplica-se a todos os dados pessoais tratados pela organização, independentemente do meio (físico ou digital), e a todos os colaboradores, prestadores de serviços e terceiros que tenham acesso a esses dados. Abrange incidentes de segurança que resultem em violação de dados pessoais, incluindo acesso não autorizado, destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito de dados pessoais.

Av. Dr. Lauro Vieira Chaves, 1030 - Vila União
CEP: 60422-901 • Fortaleza / CE
CNPJ: 07.040.108/0001-57

5 OBJETIVOS

5.1 Definir procedimentos e responsabilidades para a detecção de violações de dados pessoais.
5.2 Estabelecer diretrizes para a análise de incidentes de violação de dados pessoais.
5.3 Determinar as ações para a contenção de violações de dados pessoais.
5.4 Orientar a erradicação das causas de violações de dados pessoais.
5.5 Abordar as atividades de pós-incidente de violações de dados pessoais.
5.6 Minimizar os impactos de incidentes de privacidade e proteção de dados.
5.7 Garantir a conformidade legal e regulatória com a Lei Geral de Proteção de Dados (LGPD).
5.8 Proteger os direitos e liberdades dos titulares de dados.
5.9 Preservar a reputação da organização.
5.10 Evitar sanções legais e financeiras

6 PROCESSO DE GESTÃO DE INCIDENTES DE SEGURANÇA E PRIVACIDADE DE DADOS PESSOAIS

6.1. PREPARAÇÃO

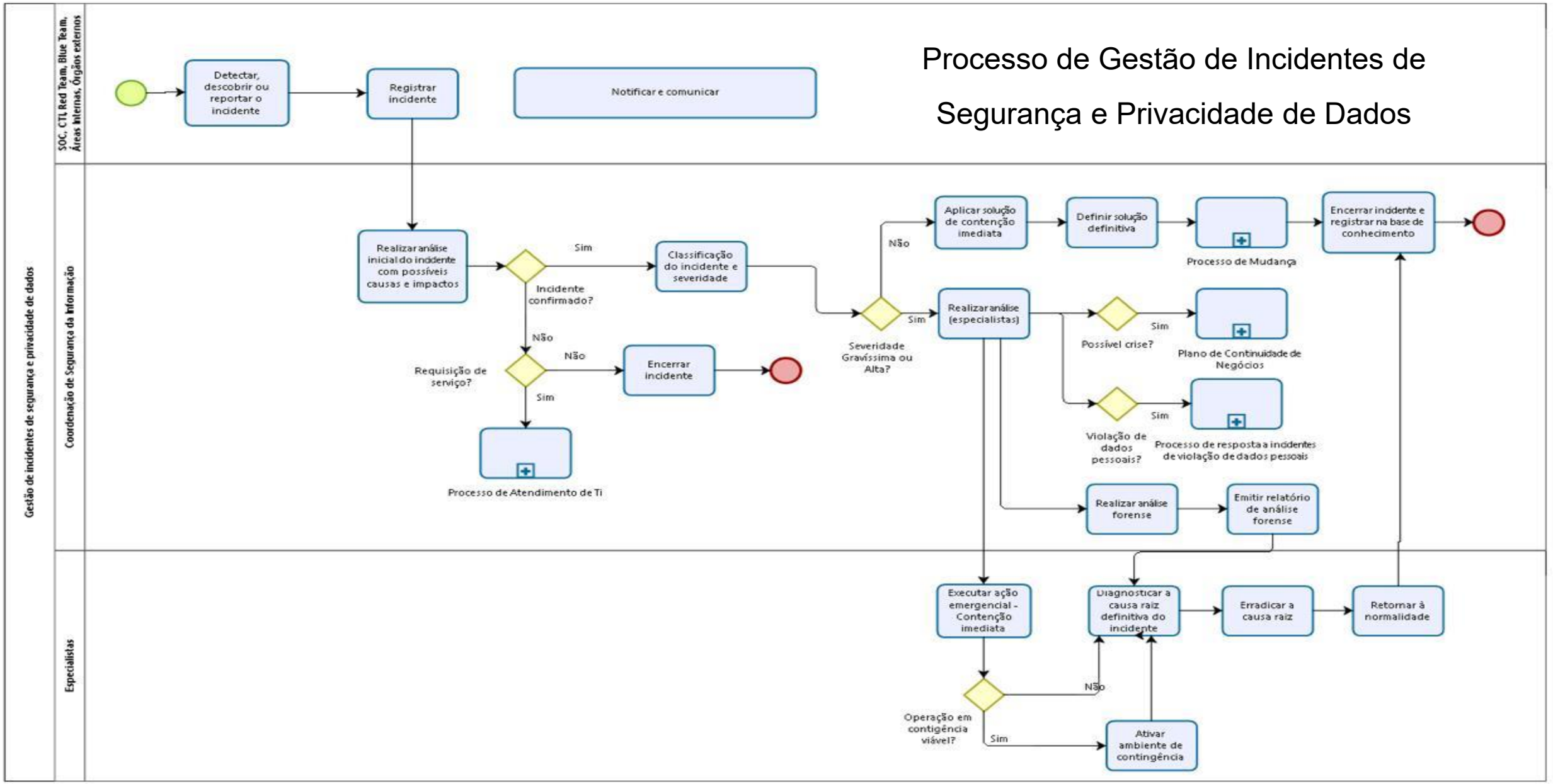
Esta fase é contínua e envolve todas as atividades preventivas e de planejamento para garantir que a organização esteja pronta para responder a um incidente. Inclui:

6.1.1 **POLÍTICAS E PROCEDIMENTOS**: Desenvolvimento e manutenção de políticas de segurança da informação e privacidade, e procedimentos detalhados para a gestão de incidentes.
6.1.2 **TREINAMENTO E CONSCIENTIZAÇÃO**: Treinamento regular de todos os colaboradores sobre a LGPD, segurança da informação e procedimentos de reporte de incidentes.
6.1.3 **FERRAMENTAS E TECNOLOGIAS**: Implementação e manutenção de ferramentas de segurança (firewalls, antivírus, SIEM, etc.) e tecnologias de proteção de dados (criptografia, anonimização, pseudonimização).
6.1.4 **PLANO DE COMUNICAÇÃO**: Definição de canais e modelos de comunicação para notificação de incidentes à ANPD e aos titulares.
6.1.5 **TESTES E SIMULAÇÕES:** Realização periódica de testes e simulações de incidentes para avaliar a eficácia do PRI e identificar pontos de melhoria.

6.2. DETECÇÃO E ANÁLISE

Esta fase inicia-se com a identificação de um evento que pode indicar um incidente de segurança ou privacidade.

Processo de Gestão de Incidentes de Segurança e Privacidade de Dados



POPCOM299

Cagece **Procedimento Operacional** CEARÁ GOVERNO DO ESTADO

Título:	Código	Versão	Página
Tratamento de Dados Pessoais pelo Atendimento Presencial e Telefônico	POPCOM299	02	1/6

1.Objetivo
1.1 Descrever o procedimento de Tratamento de Dados Pessoais pelo Atendimento Presencial e Telefônico, que se refere a impossibilitar o uso indevido de dados pessoais no processo de atendimento ao cliente externo em cumprimento à Lei Geral
nº 13.709/2018.

2.Campo de Aplicação
2.1 Atendimento Presencial – realizado pela Loja/Núcleo/Gecli;
2.2 Atendimento Telefônico – realizado pela Central de Atendi

3.Conceitos
3.1 **LGPD:** Lei Geral de Proteção de Dados, de nº 13.709/2018
3.2 **Documento:** Unidade de registro de informações, qualque
3.3 **Dado Pessoal:** É toda informação que permite identific
indivíduo que esteja vivo (pessoa natural), tais como nome,
nascimento, telefone, endereço residencial, localização via G
histórico de pagamentos, hábitos de consumo, endereço de
outros;
3.4 **Dado Pessoal Sensível:** É quando o dado for sobre or
religiosa, opinião política, filiação a sindicato ou a organizaç
ou político, dado referente à saúde ou à vida sexual, dado
vinculado a uma pessoa natural;
3.5 **Tratamento de Dados Pessoais:** É qualquer atividade
execução da sua operação, como, por exemplo: coleta, pr
utilização, acesso, reprodução, transmissão, distribuição,
armazenamento, eliminação, avaliação ou controle da inform
transferência, difusão ou extração;
3.6 **Titular**: Pessoa natural a quem se referem os dado
tratamento;
3.7 **Procurador:** Pessoa capaz e de sua confiança que é nc
(procurador), para agir em seu nome em determinada situa
possa estar presente;
3.8 **Procuração:** É um instrumento formal e legal no qual u
em seu nome;
3.9 **Termo de curatela**: termo emitido por meio de decisão
será o responsável (curador), pela pessoa natural julgada inca
que não conseguem expressar sua vontade nem praticar atos
3.10 **Curador:** É o responsável por gerir os bens do curatelad
3.11 **Termo de Inventário**: termo emitido por meio de de
quem será o responsável (inventariante) para administrar e r
bens, direitos e obrigações deixados pelo falecido) durante to
3.12 **Anonimização:** É a utilização de meios técnicos razoáv
tratamento, por meio dos quais um dado perde a possibi
indireta, a um indivíduo/pessoa natural;
3.13 **Controlador:** No âmbito da LGPD, é a pessoa natural
privado, a quem competem as decisões referentes ao tratam

Documento controlado conforme P

Cagece **Procedimento Operacional** CEARÁ GOVERNO DO ESTADO

Título:	Código	Versão	Página
Tratamento de Dados Pessoais pelo Atendimento Presencial e Telefônico	POPCOM299	02	2/6

a Cagece;
3.14 **Operador:** No âmbito da LGPD, é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, no caso o

4. Características Gerais

4.1 Apenas o titular dos dados pessoais/procurador poderá, a partir de sua identificação formal, obter informações/acesso aos dados registrados em nossos sistemas. A exceção acontece quando o cliente não é o titular/procurador, mas fornece os dados pessoais do titular e, neste caso, poderá ser esclarecido exclusivamente sobre o cálculo dos valores que compõem a fatura ou entregue a 2ª via da fatura e/ou a Certidão Negativa;

4.2 Todo dado pessoal tratado pelos processos e/ou sistemas deve ser pertinente e limitado em relação aos fins para os quais será utilizado, ou seja, não pode ser compartilhado com terceiros sendo de uso exclusivo do titular/procurador e do operador durante o atendimento;

4.3 O tratamento de documento que contenha dados pessoais deve respeitar as regras de privacidade e proteção de dados definidas na Norma Interna de Segurança e Privacidade de Dados, do Sistema de Planejamento (NIG-0032);

4.4 Os dados pessoais solicitados para atendimento de um dos serviços da Cagece são para a criação de Contrato de Prestação de Serviço, atualização/correção de cadastro do cliente, faturamento e arrecadação, bem como, para o cumprimento à legislação aplicada;

4.5 É proibido deixar exposto nas mesas e ambiente de trabalho qualquer documento físico que tenha dados pessoais;

4.6 O armazenamento de dados pessoais em meio físico deve ser em local seguro onde apenas pessoas envolvidas em seu tratamento possam ter acesso, devendo serem utilizadas gavetas ou armários trancados;

4.7 Os dados em meio digital devem ser armazenados exclusivamente em nossos sistemas e/ou servidor. Jamais devem ser salvos em dispositivos de armazenamento como Disco Rígido, CD, CD-R, CD-RW, DVD, HD DVD, SSD, Cartão de Memória e Pen Drive (USB), Armazenamento em Nuvem, entre outros;

ACORDO INDIVIDUAL DE TRATAMENTO DE DADOS PESSOAIS NA PRESTAÇÃO DE SERVIÇOS

ACORDO INDIVIDUAL DE TRATAMENTO DE DADOS PESSOAIS NA PRESTAÇÃO DE SERVIÇOS

CONTRATADA: [Identificação completa da empresa prestadora contratada]

EMPREGADO(A) DA CONTRATADA: [Nome completo e qualificação completa do empregado(a) da CONTRATADA].

(i) Considerando o contrato [Número do contrato] firmado entre ~~o CONTRATADA~~ e a Companhia de Água e Esgoto do Ceará – CAGECE;

(ii) Considerando que, em [data do contrato original], o(a) EMPREGADO(A) DA CONTRATADA foi contratado(a) como funcionário da CONTRATADA para prestar serviços à Companhia de Água e Esgoto do Ceará – CAGECE;

(iii) Considerando que em razão da contratação acima referida o EMPREGADO(A) DA CONTRATADA terá acesso a Dados Pessoais, assim consideradas quaisquer informações relacionadas à pessoa natural identificada ou identificável de clientes, colaboradores ou terceiros da Companhia de Água e Esgoto do Ceará – CAGECE;

(iv) Considerando ser necessária a definição de regras e critérios para o tratamento de Dados Pessoais, em respeito ao que estabelece a Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD).

As partes acima acordam o seguinte:

1. DEFINIÇÕES A RESPEITO DO TRATAMENTO DE DADOS PESSOAIS PELO(A) EMPREGADO(A) DA CONTRATADA.

1.1. O(A) EMPREGADO(A) DA CONTRATADA declara estar ciente de que a CAGECE mantém políticas de privacidade e proteção de dados pessoais e que é seu dever conhecê-los e cumpri-los.

1.2. O(A) EMPREGADO(A) DA CONTRATADA se compromete a:

1.2.1. Atender de modo diligente às orientações prestadas e às solicitações formuladas pelo Encarregado de Proteção de Dados Pessoais (EPD) da instituição contratante, relativamente ao tratamento de Dados Pessoais, o que deverá fazer no prazo que lhe for assinalado, apresentando, sempre que lhe for exigida, a evidência respectiva de conformidade.

1.2.2. Tratar os Dados Pessoais que lhe forem confiados exclusivamente para atender às finalidades e de acordo com as instruções definidas pela CAGECE e pela CONTRATADA.

1.2.3. Acessar apenas os Dados Pessoais relacionados às atividades que lhe competem em razão de seu cargo ou função, comunicando ao EPD caso verifique que lhe foi concedido acesso indevido a outros Dados Pessoais.

1.2.4. Certificar-se de que os funcionários que lhe sejam eventualmente subordinados, tenham acesso aos Dados Pessoais estritamente necessários para o cumprimento das atividades inerentes a seus cargos/funções.

1.2.5. Armazenar Dados Pessoais de acordo com as diretrizes traçadas pela CAGECE e pela CONTRATADA.

1.2.6. Não compartilhar Dados Pessoais senão nas hipóteses estabelecidas pela CAGECE e/ou pela CONTRATADA.

Av. Dr. Lauro Vieira Chaves, 1030 - Vila União
CEP: 60422-901 • Fortaleza / CE
CNPJ: 07.040.108/0001-57

1.2.7. Respeitar o dever de confidencialidade de Dados Pessoais.

1.2.8. Comunicar de pronto ao gestor imediato quaisquer fatos que, segundo sua percepção, impliquem em violação ou ameaça de violação à privacidade ou à segurança dos Dados Pessoais e que possam acarretar risco ou dano relevante aos seus titulares.

1.2.9. Cooperar com a realização de auditorias ou inspeções relacionadas ao tratamento de Dados Pessoais eventualmente realizadas pela CAGECE.

1.2.10. Respeitar as medidas técnicas e administrativas definidas pela CAGECE e pela CONTRATADA para a proteção de Dados Pessoais.

2. DEFINIÇÕES A RESPEITO DO TRATAMENTO DE DADOS PESSOAIS DO(A) EMPREGADO(A) DA CONTRATADA.

2.1. Em virtude da relação contratual havida entre a CONTRATADA e a CAGECE, esta poderá realizar o tratamento dos seguintes Dados Pessoais do EMPREGADO(A) DA CONTRATADA: nome completo; estado civil; e-mail; telefone; endereço; filiação paterna; filiação materna; idade; gênero; data de nascimento; RG; CPF; PIS; CTPS; título de eleitor; carteira de reservista; dados pessoais bancários; fotografia para uso cadastral; escolaridade; nome completo de dependentes; data de nascimento de dependentes; cargo ocupado na instituição; carga horária inerente ao cargo; número de matrícula; experiências profissionais anteriores (salários, cargos ocupados, instituições às quais foi vinculado, tempo de permanência em outras instituições, data de admissão, data de desligamento etc.); estado de saúde atualizado e diagnósticos; perfis social e profissional; informações inerentes à avaliação funcional (competências, notas obtidas em suas avaliações, comentários sobre competências).

2.2. A CAGECE poderá realizar operações de tratamento de Dados Pessoais comuns/gerais do EMPREGADO(A) DA CONTRATADA, independentemente de seu consentimento, para:

(i) Cumprir obrigações legais ou regulatórias que lhe sejam impostas;

(ii) O exercício regular de direitos em eventual processo judicial ou arbitral;

(iii) A proteção da vida ou da incolumidade física do(a) EMPREGADO(A) DA CONTRATADA ou de ~~terceiro~~;

2.3. A CAGECE somente poderá realizar operações de tratamento de Dados Pessoais comuns/gerais do(a) EMPREGADO(A) DA CONTRATADA para finalidades não indicadas nos itens 2.1 e 2.2, mediante o seu consentimento livre, informado e inequívoco.

2.4. A CAGECE poderá realizar operações de tratamento de Dados Pessoais Sensíveis do EMPREGADO(A) DA CONTRATADA (assim compreendidos aqueles relacionados à origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico) independentemente do seu consentimento, para:

(i) Cumprir obrigações legais ou regulatórias que lhe são ou serão impostas;

(ii) O exercício regular de direitos em eventual processo judicial ou arbitral;

(iii) Proteção da vida ou da incolumidade física do(a) EMPREGADO(A) DA CONTRATADA ou de ~~terceiro~~;

Av. Dr. Lauro Vieira Chaves, 1030 - Vila União
CEP: 60422-901 • Fortaleza / CE
CNPJ: 07.040.108/0001-57

2.5. A CAGECE somente poderá realizar operações de tratamento de Dados Pessoais Sensíveis do(a) EMPREGADO(A) DA CONTRATADA, para finalidades não indicadas no item anterior, mediante o seu consentimento livre, informado e inequívoco.

2.6. A CAGECE poderá realizar auditorias no e-mail corporativo (correio eletrônico), aplicativos próprios ou outros meios de comunicação oficiais utilizados pelo(a) EMPREGADO(A) DA CONTRATADA, tendo em vista se tratar de um instrumento de trabalho.

2.7. A CAGECE e a CONTRATADA responsabilizam-se pela manutenção de medidas técnicas e administrativas de segurança aptas a proteger os Dados Pessoais de qualquer forma de tratamento inadequado ou ilícito;

3. OUTRAS DISPOSIÇÕES

3.1. E por estarem acordados, firmam o presente instrumento em 02 (duas) vias de igual teor e forma.

Fortaleza, Ceará, [data].

Plano de Cibersegurança

Proteção contra ameaças externas

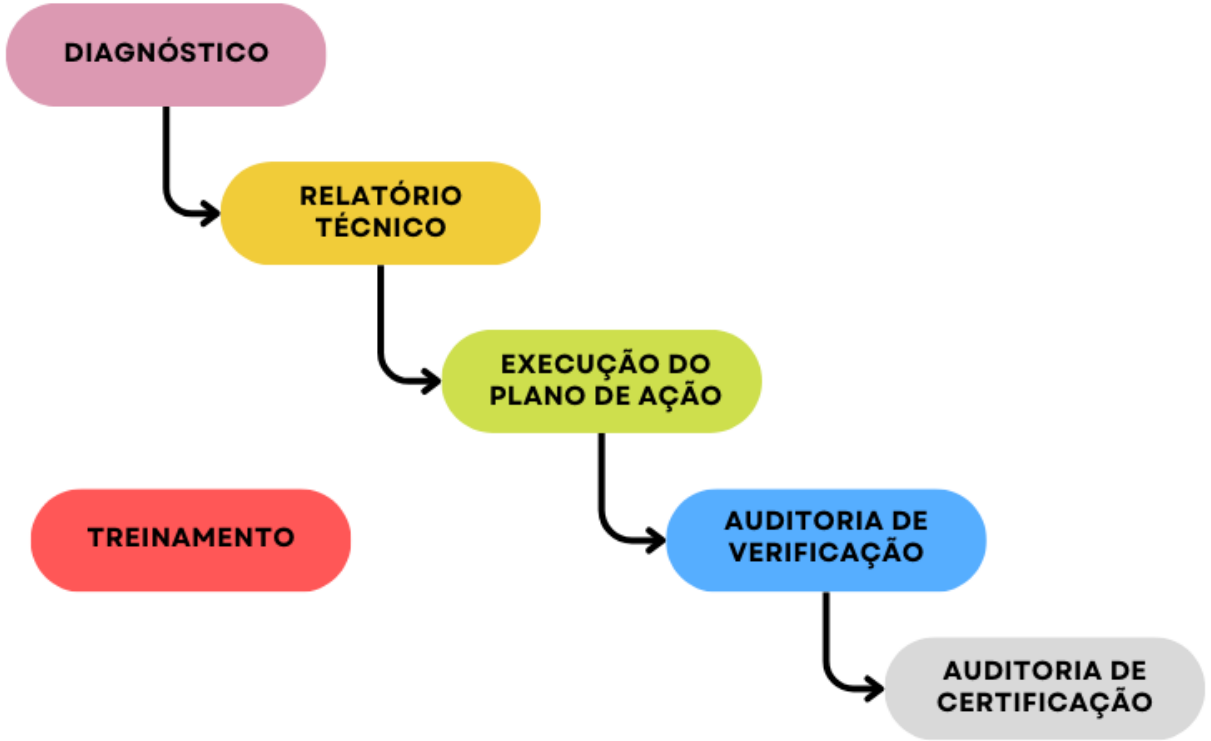
Invasão de hackers, bots, scripts automatizados;

Proteção contra ameaças internas

Erro humano, funcionários mal intencionados;

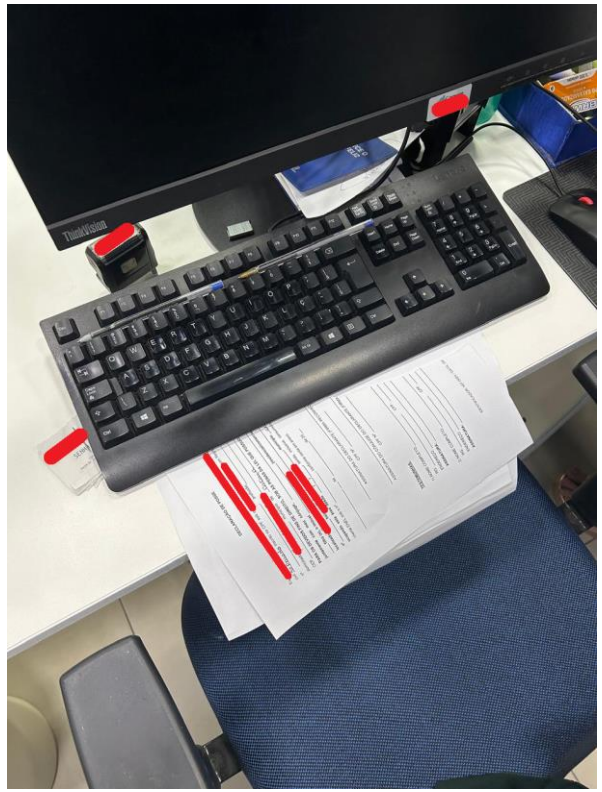
Proteção e controle de acessos privilegiados

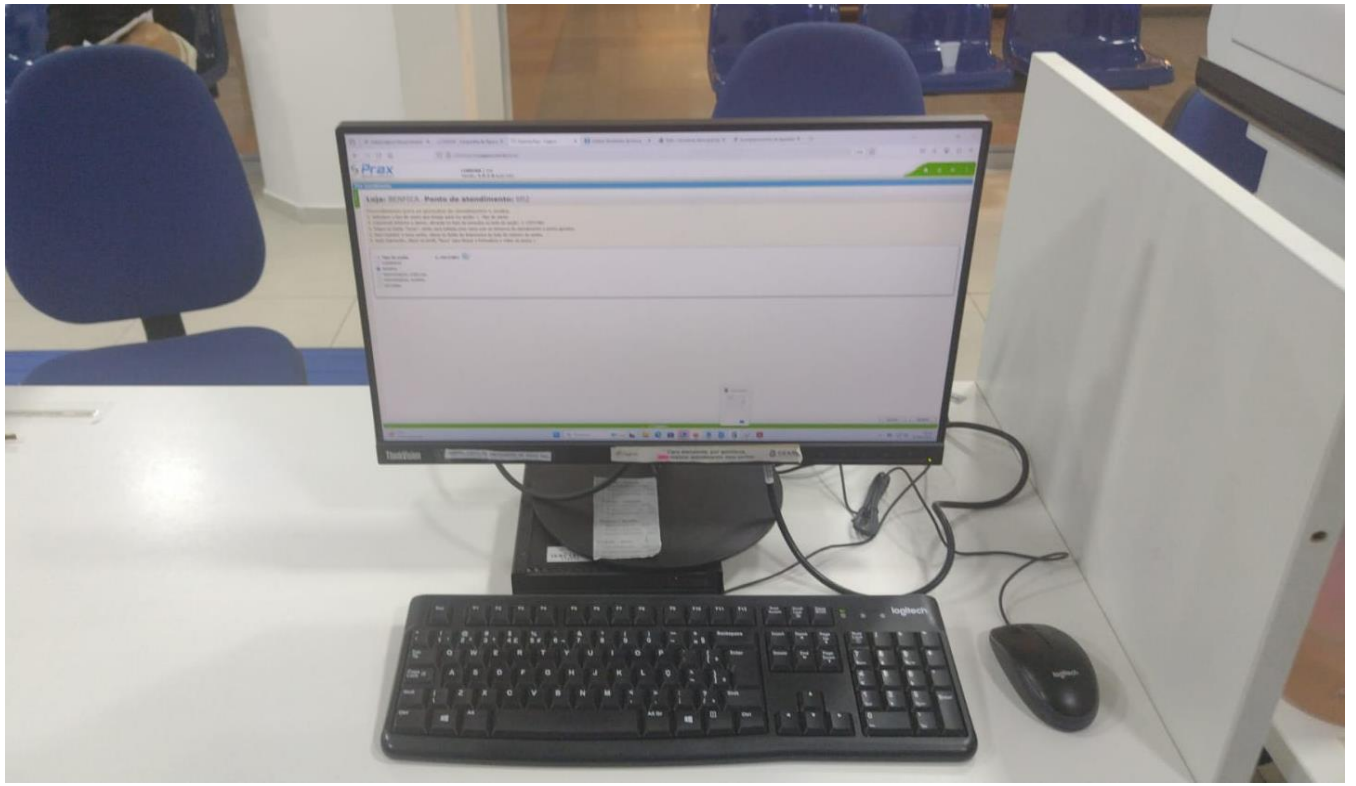
Certificação ISO/IEC 27001:2022



TÉCNICO	GOVERNANÇA	OPERACIONAL	ADMINISTRATIVO	PLANEJAMENTO E MELHORIA
• Controle de Acesso • Criptografia • Segurança em Operações • Segurança em Comunicações • Aquisição, Desenvolvimento e Manutenção de Sistemas	• Políticas de Segurança da Informação • Organização da Segurança da Informação • Aspectos de Segurança da Informação na Gestão da Continuidade de Negócios • Conformidade	• Gerenciamento de Ativos • Segurança Física e Ambiental • Gestão de Incidentes de Segurança da Informação	• Segurança em Recursos Humanos • Relações com Fornecedores	• Planejamento e Melhoria

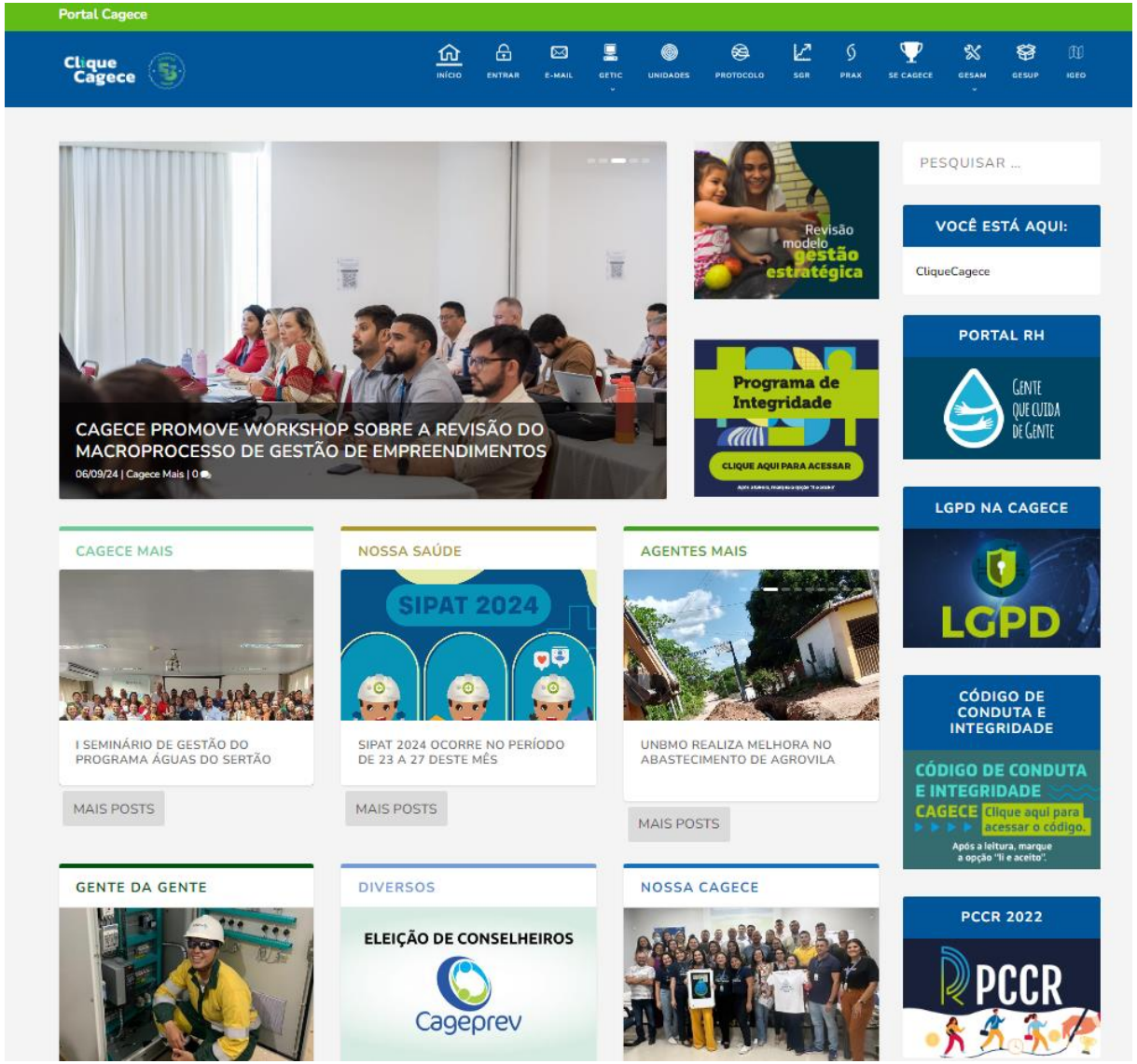
Medidas de privacidade





Medidas de privacidade

Medidas de Privacidade



Proteção física

Controles de Privacidade de Dados
Due Diligence

Item		SIM/ NÃO/ PARCIALMENTE	DESCREVER COM DETALHAMENTO
1	**PRIVACIDADE DE DADOS**		
1.1	Existe um encarregado de proteção de dados (DPO) ?		
1.2	Existe política para proteção de dados e privacidade ?		
1.3	Mantém plano de resposta a demandas de titulares ?		
1.4	Mantém plano de resposta a incidentes de violação de dados ?		
1.5	Mantém registro das operações que envolvam dados pessoais ?		
1.6	Mantém processo de notificação de incidentes de violação de dados ?		
1.7	Mantém uma cultura de privacidade de dados (comunicação, educação, treinamento, conscientização e sensibilização dos colaboradores) ?		
1.8	Avalia impacto de privacidade quando novos tratamentos ou mudanças de tratamento de dados pessoais que sejam críticos/sensíveis/ ou em larga escala ?		
1.9	Implementa a Privacidade por Design e por Default ou Privacy by Design and Default para os serviços com tratamento de dados, seja no mundo físico ou virtual, tenha como base respeito à privacidade das informações utilizadas, com ampla segurança de dados		
1.10	Utiliza criptografia de dados e/ou anonimização dos dados ?		
1.11	Mantém algum subcontratado com tratamento de dados pessoais ?		
1.12	Mantém políticas, procedimentos e/ou mecanismos documentados para o descarte de dados pessoais ?		
1.13	São utilizados termos de confidencialidade para colaboradores que realizam tratamento dos dados pessoais?		

Controles de Privacidade de Dados
Due Diligence

Item		SIM/ NÃO/ PARCIALMENTE	DESCREVER COM DETALHAMENTO
2	**SEGURANÇA DA INFORMAÇÃO**		
2.1	Existe política de segurança da informação ?		
2.2	Existe uma equipe dedicada à Segurança da Informação?		
2.3	Mantém processo de notificação de incidentes de segurança ?		
2.4	São instalados firewalls entre os ambientes de redes distintos (redes, redes sem fio e internet) ?		
2.5	São utilizados sistemas de detecção e prevenção de invasões (rede e/ou local) e as assinaturas e anomalias são atualizadas periodicamente?(ex: IDS/IPS)		
2.6	Mantém uma cultura de segurança da informação (comunicação, educação, treinamento, conscientização e sensibilização dos colaboradores) ?		
2.7	Utiliza antivírus atualizado em todos os computadores/servidores ?		
2.8	São realizadas Pentests (testes de invasão) ao menos anualmente?		
2.9	Possui um ambiente de alta disponibilidade (H.A – high availability) com redundância capaz de garantir a continuidade de serviços utilizados, mesmo em ocasiões de falhas (por exemplo, de hardware, software, interrupção de energia etc.) ?		
2.10	Existe plano de recuperação de desastres (DRP) ?		
2.11	Possui trilha de auditoria ?		
2.12	O sistema operacional é mantido atualizado?		
2.13	Possui autenticação de múltiplo fator ?		
2.14	Existe processo de revisão de credenciais de acesso realizado em intervalos de até 90 dias?		
2.15	Nos últimos três anos, sofreu qualquer invasão de sistema, negação de serviço (DDoS) ,Ransomware, furto de dados ou outras perdas de dados?		

Auditoria de Conformidade com a LGPD

Checklist de Auditoria de Conformidade com a LGPD

Unidade:	Site/Coordenadoria:	Data:
GEREM	Gerem Cor	09/09/24

Área auditada

ITS CUSTOMER SERVICE CNPJ 16.853.728/0007-91 - Empresa contratada do serviço de teleatendimento

Equipe Auditada:

Equipe Auditores:

Respondeu Questionário de Diligência:

( ) SIM ( ) Não Obs:

Requisitos

1. Conhecimento da LGPD	**Respostas**
1.1 O que é a LGPD para você?	
1.2 Qual a importância da LGPD?	
1.3 Dê exemplos de dados pessoais e dados pessoais sensíveis dos clientes da Cagece	
1.4 Quais os direitos dos titulares de dados?	
1.5 Quais riscos no tratamento de dados pessoais?	
2. Conscientização e capacitação em LGPD	**Respostas**
2.1 Qual treinamento você fez sobre a LGPD?	Evidenciar treinamento (certificado, frequencia...)
2.2 Quais comunicados ou informativos foram passados para os colaboradores sobre a LGPD?	
3. Normativos internos da LGPD (DPO/EPD, Política, Norma, etc)	**Respostas**
3.1 Apresentar os normativos internos sobre a LGPD	Informar normativos da contratada
4. Atuação do DPO/EPD – Encarregado de proteção de dados	**Respostas**
4.1 Quem é o DPO/EPD?	Da contratada
4.2 Qual a atuação do DPO?	Da contratada
5. Ciclo de vida dos dados pessoais (coleta, processamento, análise, compartilhamento, armazenamento, reutilização e eliminação)	**Respostas**
5.1 Os dados dos clientes recebidos por você são salvos em qual lugar?	
5.2 Como ocorre o compartilhamento de dados?	
5.3 Manuseia algum papel com dados de clientes?	
5.4 Como é feito o descarte desses papéis?	
6. Utilização de métodos e práticas	**Respostas**

Checklist de Auditoria de Conformidade com a LGPD

Unidade:	Site/Coordenadoria:	Data:
GEREM	Gerem Cor	09/09/24

Área auditada

ITS CUSTOMER SERVICE CNPJ 16.853.728/0007-91 - Empresa contratada do serviço de teleatendimento

Equipe Auditada:

Equipe Auditores:

Respondeu Questionário de Diligência:

( ) SIM ( ) Não Obs:

Requisitos

9. Ambiente de trabalho	**Respostas**
9.1 Guarda de documentos	
9.2 Mesa limpa	
9.3 Controle físico de acesso	
10. Observações Gerais	**Respostas**

Auditoria de Conformidade – LGPD (Loja de Caucaia)

Assunto: Auditoria de Conformidade com a LGPD

Data: 24/06/2025

Local: Loja de Caucaia

Participantes: Integrantes do Escritório de Privacidade e Proteção de Dados, equipe da GEREM e supervisora da Loja de Atendimento de Caucaia

Pautas:

- Educação e conscientização
- Adequação a política e norma de de privacidade
- Medidas de privacidade e proteção de dados pessoais
- Segurança física e digital dos dados
- Identificação de vulnerabilidades e riscos
- Exposição de dados pessoais
- Descarte seguro de dados pessoais
- Oportunidades de melhorias

Auditoria de Conformidade – LGPD
Prestador de Serviços – FIMM Brasil

Assunto: Auditoria de Conformidade com a LGPD

Data: 27/06/2025

Local: FIMM Brasil

Participantes: Integrantes do Escritório de Privacidade e Proteção de Dados, participantes da GETIC e GECAD, equipe da FIMM Brasil, Comitê de Privacidade e DPO da FIMM Brasil

Pautas:

- Educação e conscientização
- Adequação a política e norma de de privacidade
- Medidas de privacidade e proteção de dados pessoais
- Segurança física e digital dos dados
- Identificação de vulnerabilidades e riscos
- Exposição de dados pessoais
- Descarte seguro de dados pessoais
- Oportunidades de melhorias

Capacitação, conscientização e sensibilização

Clique Cagece

INÍCIO ENTRAR E-MAIL GETIC UNIDADES PROTOCOLO SGR PRAX

QUER SABER MAIS? CONFIRA O MATERIAL QUE TEMOS PARA VOCÊ

CAGECE CONCLUI PRIMEIRO CICLO DE WORKSHOP SOBRE LGPD DE 2022

CAGECE DÁ CONTINUIDADE ÀS CAPACITAÇÕES SOBRE LGPD PARA COLABORADORES

CAGECE CRIA ESCRITÓRIO DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

LGPD: CAGECE ELABORA RESOLUÇÃO DE DIRETORIA REFERENTE A ADITIVO DE CONTRATOS

CAGECE LANÇA SUA POLÍTICA GERAL DE PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

LGPD: CAGECE CRIA TERMO DE AUTORIZAÇÃO/CONSENTIMENTO DE USO DE IMAGEM

VEJA TODAS AS MATÉRIAS

Convocação

Convocamos todos os superintendentes, gerentes e assessores para uma reunião sobre a Lei Geral de Proteção de Dados - LGPD a ser realizada no dia 25/11, das 8h30 às 11h, de forma virtual no Teams.

Na oportunidade, haverá a **apresentação de medidas técnicas e administrativas que a Cagece vem adotando** e uma palestra intitulada **"Conhecendo a Lei Geral de Proteção de Dados - LGPD"** com o palestrante Alexandre Pinheiro, diretor de CyberSecurity, Inovação e Educação do Grupo Energy Telecom e diretor de Pesquisa, Ciência, Tecnologia e Inovação do Instituto CTEM+.

LEI GERAL DE PROTEÇÃO DE DADOS

25/11
8h30-11h
Evento virtual no Teams

No dia do evento, clique aqui para acessar a reunião virtual

Atenciosamente,
Diretoria Executiva

Cagece Governo do Estado do Ceará Secretaria das Cidades

VÍDEOS DOS WORKSHOPS

Para instruir os colaboradores sobre a LGPD, foram realizados workshops on-line.

A gravação desses workshops estão disponibilizadas na plataforma de EAD da Cagece e você pode acessá-las clicando sobre as imagens abaixo.

Para assistir aos vídeos, você precisa acessar a plataforma (login e senha de rede) e usar a chave: **LGPD2022**

PROCESSOS E RESULTADOS CORPORATIVOS

Clique para acessar a plataforma

SEGURANÇA DE DADOS E DOMÍNIO PÚBLICO

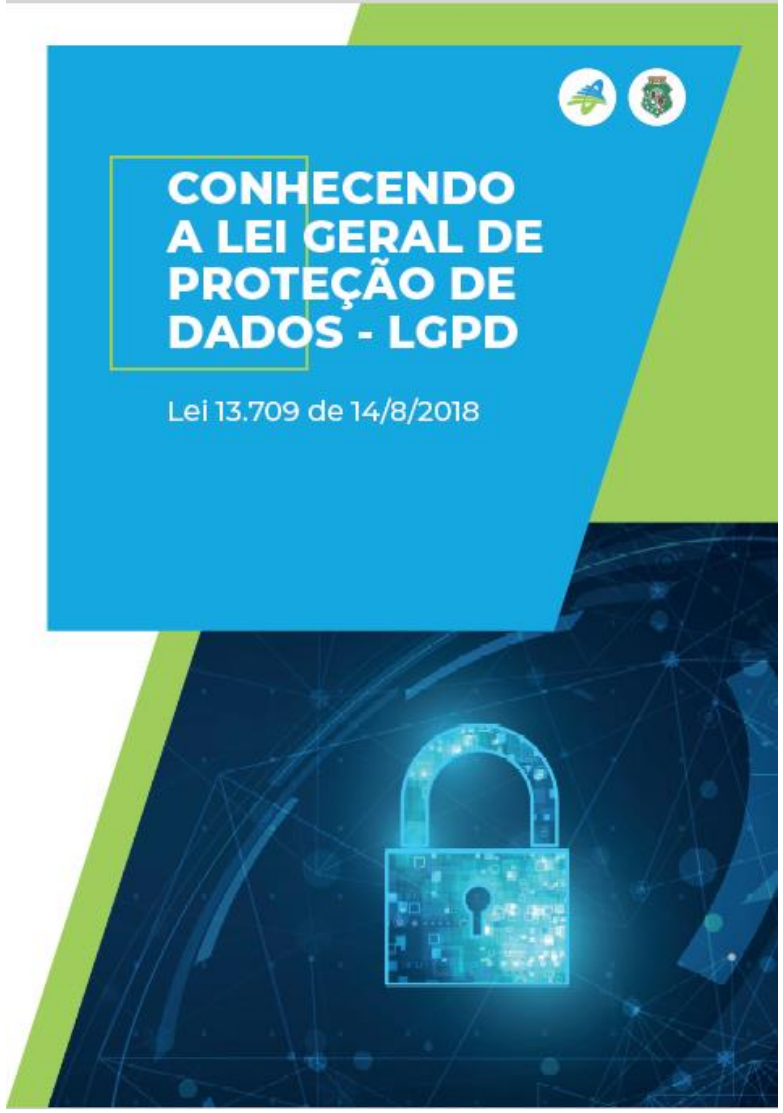
Clique para acessar a plataforma

ATENDIMENTO DE DIREITOS DE TITULARES DE DADOS

Clique para acessar a plataforma

EXIN Data Protection Officer
EXIN CERTIFIED

Cartilha



SUMÁRIO

4.14 Colaboradores da companhia

– A leitura, ciência e cumprimento dessa norma;

– Adotar medidas de segurança e privacidade de dados pessoais sob sua responsabilidade, compreendendo e não se limitando a sistemas, softwares, mesa de trabalho, equipamentos de informática, telefones, documentos, relatórios, imagens, fotos, vídeos, rede de dados e divulgação de informações.

5. TRATAMENTO DE DADOS PESSOAIS

5.1 Todo processo que envolver coleta e tratamento de dados pessoais somente poderá ser realizado depois de analisado e homologado pelo encarregado dos dados DPO (Data Protection Officer);

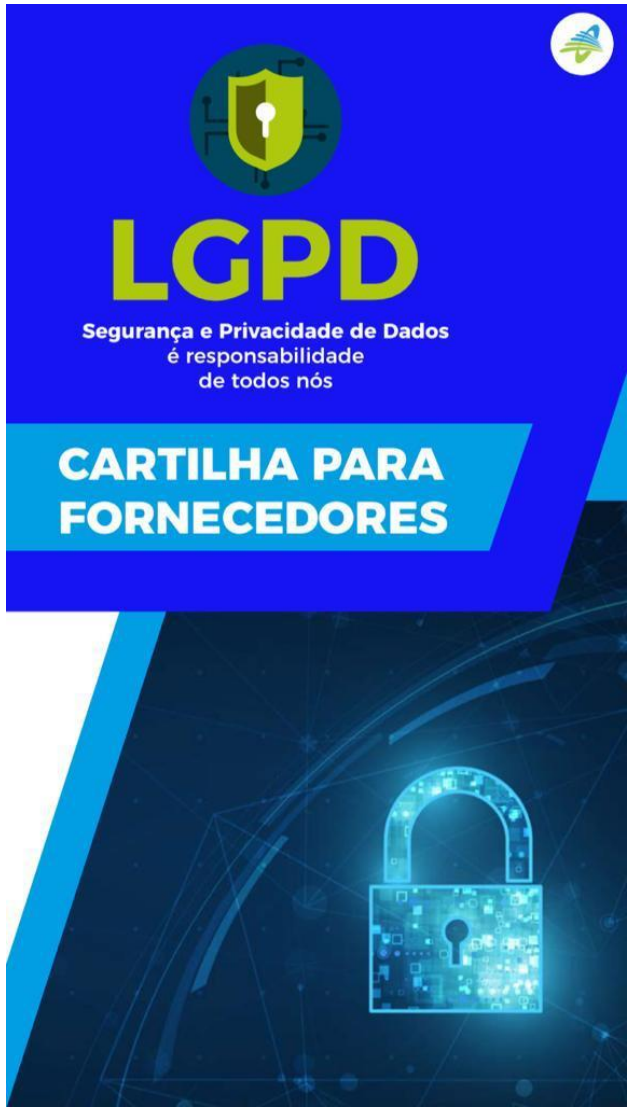
5.2 Todo sistema ou produto deve ser construído e mantido pensando na máxima proteção da privacidade dos seus usuários (Privacy by Design, Privacy by Default);

5.3 Todo processo deve ser construído obtendo o mínimo possível de dados pessoais necessários para o processo, devendo ser observado sempre seus propósitos e o legítimo interesse para sua utilização;

5.4 Os processos da companhia devem estar mapeados a utilização dos dados pessoais e seus fluxos;

5.5 A utilização de dados pessoais para a realização de estudos

Cartilha do Fornecedor



RESPONSABILIDADES DOS FORNECEDORES

O item 6.7 da PGPPDP da Cagece estabelece as seguintes responsabilidades de colaboradores e prestadores de serviços:

- Atender de modo diligente às orientações prestadas e às solicitações formuladas pelo EPD relativamente ao tratamento de dados, o que deverá fazer no prazo que lhe for assinalado, apresentando, sempre que lhe for exigida, a evidência respectiva de conformidade;
- Tratar os dados que lhe forem confiados exclusivamente para atender às finalidades e de acordo com as instruções definidas pela Cagece;
- Acessar apenas os dados relacionados às atividades que lhe competem em razão de seu cargo ou função, comunicando ao EPD caso verifique que lhe foi concedido acesso indevido a outros dados pessoais;
- Certificar-se de que os(as) empregados(as), que lhe sejam eventualmente subordinados, tenham acesso aos dados estritamente necessários para o cumprimento das atividades inerentes a seus cargos/funções;

LGPD CAGECE | FORNECEDORES

- Armazenar dados de acordo com as diretrizes traçadas pela Cagece;
- Não compartilhar dados senão nas hipóteses estabelecidas pela Cagece;
- Respeitar o dever de confidencialidade dos dados;
- Comunicar imediatamente ao EPD quaisquer fatos que, segundo sua percepção, impliquem em violação ou ameaça de violação à privacidade ou à segurança dos dados e que possam acarretar risco ou dano relevante aos seus titulares;
- Cooperar com atividade de auditorias ou inspeções relacionadas ao tratamento de dados pessoais eventualmente realizadas pela Cagece;
- Respeitar as medidas técnicas e administrativas definidas pela Cagece para a proteção de dados.
- Zelar pela integridade, disponibilidade, confidencialidade, autenticidade e legalidade dos dados que tratar.
- Outras obrigações definidas neste documento e outras normas internas.

Essas responsabilidades estarão previstas em cláusulas contratuais e também nos aditivos aos contratos quando as mesmas mencionarem a obrigatoriedade de atendimento à PGPPDP.

Cartilha para Atendimento ao Cliente

6. Quais são os direitos dos titulares?

A LGPD estabelece os seguintes direitos aos titulares de dados:

- Confirmação da existência do tratamento de dados;
- Acesso aos dados pelo titular;
- Correção de dados incompletos, inexatos ou desatualizados;
- Anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei;
- Portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa de acordo com a autoridade nacional, observados os segredos comercial e industrial;
- Eliminação dos dados tratados com consentimento do titular, salvo as hipóteses previstas no art. 16 da LGPD, ou seja, ter ciência (ou anuência) da eliminação dos seus dados após o término de seu tratamento (grifo nosso);
- Revogação do consentimento nos termos do § 5º do art. 8º;
- Informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados;
- Informação sobre a possibilidade de não fornecer consentimento sobre as consequências da negativa.

7. Orientações gerais

A Política de Privacidade e Proteção de Dados Pessoais (PPPDP) estabelece princípios, regras, diretrizes, atribuições e responsabilidades relativamente à gestão de dados pessoais no âmbito da Cagece, sendo aplicável a colaboradores, fornecedores, prestadores de serviços e parceiros.

A política está disponível no link: ***www.cagece.com.br/politica-de-privacidade***

Todos os fornecedores, parceiros e demais entidades que possam coletar, armazenar ou tratar dados pessoais de clientes ou colaboradores da companhia deverão estar de acordo com os requisitos de privacidade e proteção de dados das normas e políticas da Cagece.

Todos os colaboradores devem zelar pelas informações tratadas, mantendo o sigilo e a segurança dos documentos manuseados. Para isso, são necessários os seguintes cuidados:

a) organizar e limpar diariamente as estações de trabalho, de modo que toda a documentação seja guardada em local seguro, como armários fechados com chave, gavetas trancadas etc;

b) garantir que os documentos a serem arquivados temporariamente não fiquem expostos e sejam prontamente guardados em armários com chave;

c) garantir que as chaves de armários e mesas sejam guardadas em local específico e apropriado;

d) evitar impressões em papel e utilizar prioritariamente impressões em meio digital com armazenamento seguro;

e) salvar arquivos, documentos com dados pessoais somente no servidor de arquivos para acesso controlado;

Ações de Comunicação e Conscientização

Forum GETER

Assunto: Apresentação das Práticas da Cagece de Privacidade e Proteção de Dados

Data: 24/06/2025

Local: Auditório do Corpo dos Bombeiros

Participantes: Integrantes do Escritório de Privacidade e Proteção de Dados, equipe da Gerência de Terceirização, colaboradores representantes das empresas terceirizadas de mão de obra

Pautas:

- Conceitos, dados sensíveis e dicas de proteção
- Plano de Resposta a Incidentes de Privacidade
- Escritório de Privacidade e Proteção de Dados Pessoais
- Ações de comunicação, conscientização e sensibilização dos colaboradores
- Acordo Individual de Tratamento de Dados Pessoais na Prestação de Serviços
- Controles de Privacidade de Dados (Due Diligence)
- Auditoria de Conformidade com a LGPD

Dia D - LGPD com Supervisores de Loja de Atendimento

Assunto: Apresentação das Práticas da Cagece de Privacidade e Proteção de Dados

Data: 13/05/2025

Local: Auditório da Cagece

Palestrante: Otávio Frota

Participantes: Integrantes do Escritório de Privacidade e Proteção de Dados, equipe da GEREM, SCM e supervisores de lojas de atendimento

Pautas:

- Conceitos, dados sensíveis e dicas de proteção
- Plano de Resposta a Incidentes de Privacidade
- Escritório de Privacidade e Proteção de Dados Pessoais
- Ações de comunicação, conscientização e sensibilização dos colaboradores
- Acordo Individual de Tratamento de Dados Pessoais na Prestação de Serviços
- Controles de Privacidade de Dados (Due Diligence)
- Auditoria de Conformidade com a LGPD

Supervisores de lojas de atendimento participam de treinamento específico sobre LGPD

Para intensificar os cuidados relativos ao tratamento de dados dos clientes, o Escritório de Privacidade e Proteção de Dados, em parceria com a superintendência Comercial, promoveu no último dia 13, um treinamento para os supervisores de lojas de atendimento da Cagece. O encontro, coordenado pela Gerência de Relacionamento com o Cliente (Gerem) foi realizado no auditório da sede e contou com a participação de supervisores das lojas da capital e do interior.

Quinta do Repasse

Assunto: Apresentação das Práticas da Cagece de Privacidade e Proteção de Dados

Data: 05/06/2025

Local: Videoconferência (Google Meet)

Palestrante: Otávio Frota

Participantes: Integrantes do Escritório de Privacidade e Proteção de Dados, equipe da GDEMP e para líderes de escopo e auditores internos da qualidade

Pautas:

- Conceitos, dados sensíveis e dicas de proteção
- Plano de Resposta a Incidentes de Privacidade
- Escritório de Privacidade e Proteção de Dados Pessoais
- Ações de comunicação, conscientização e sensibilização dos colaboradores
- Acordo Individual de Tratamento de Dados Pessoais na Prestação de Serviços
- Controles de Privacidade de Dados (Due Diligence)
- Auditoria de Conformidade com a LGPD

FUNCEME

Assunto: Apresentação das Práticas da Cagece de Privacidade e Proteção de Dados

Data: 16/10/2024

Local: Auditório da Funceme

Palestrante: Otávio Frota

Participantes: Integrantes do Escritório de Privacidade e Proteção de Dados e colaboradores da Funceme

Pautas:

- Conceitos, dados sensíveis e dicas de proteção
- Plano de Resposta a Incidentes de Privacidade
- Escritório de Privacidade e Proteção de Dados Pessoais
- Ações de comunicação, conscientização e sensibilização dos colaboradores
- Acordo de Tratamento de Dados Pessoais
- Controles de Privacidade de Dados (Due Diligence)
- Auditoria de Conformidade com a LGPD

Para mais informações
Reporte de Incidentes

- ✅ Comunique de imediato o seu gestor

- ✅ Acione de imediato o EPPDP (Escritório de Privacidade e Proteção de Dados Pessoais).

- ✔ privacidadededados@cagece.com.br
- ✔ grupo.privacidadedados@cagece.com.br