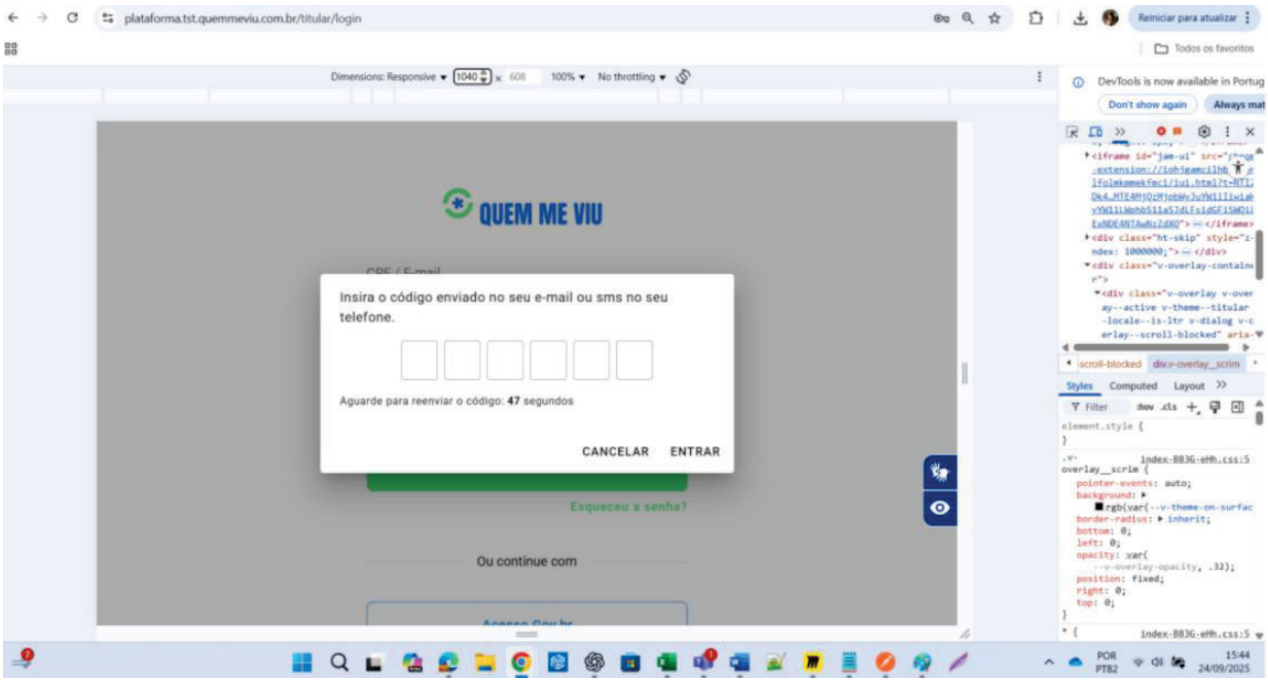
1. Descrição

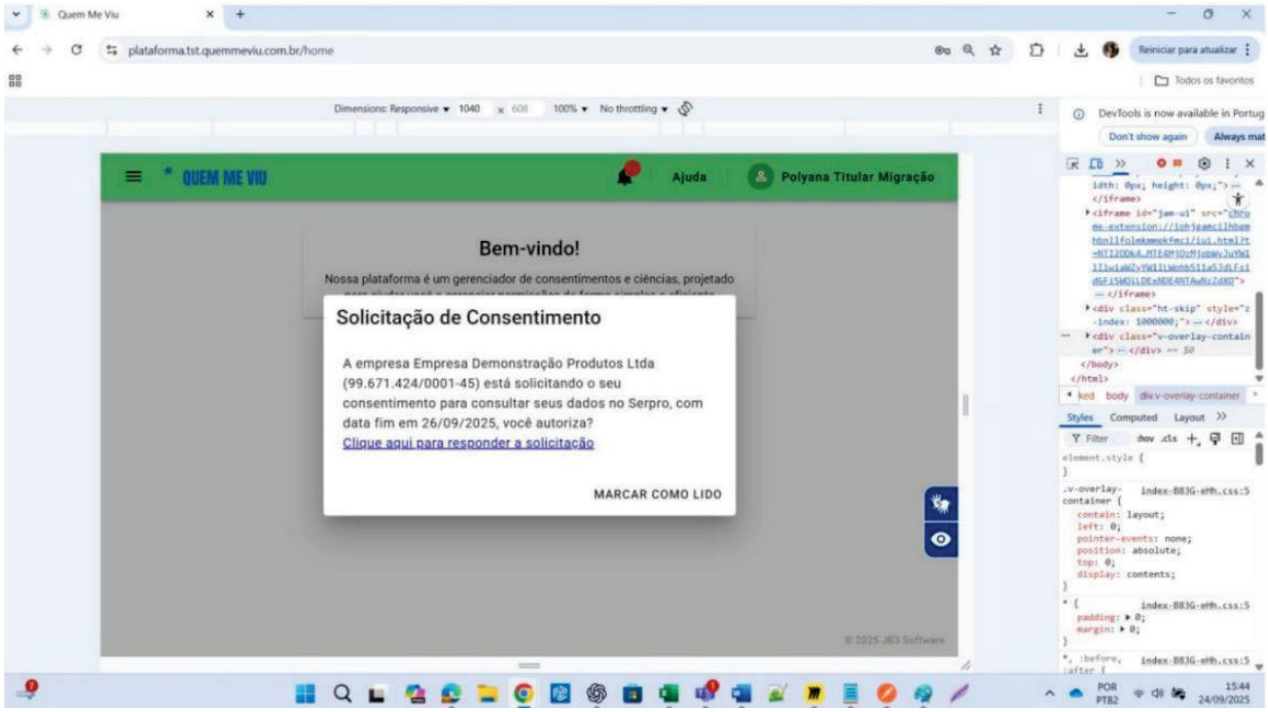
As aplicações foram desenvolvidas de forma web responsivas e mobile (iOS e Android), garantindo interfaces intuitivas, amigáveis e adaptáveis a diferentes dispositivos e tamanhos de tela. As soluções apresentam alta qualidade de UI/UX, priorizando a experiência do usuário, navegabilidade e estética. Além disso, estão em conformidade com os padrões de acessibilidade digital definidos pela WCAG 2.1, assegurando que pessoas com diferentes necessidades possam utilizar as aplicações de forma inclusiva e eficiente.

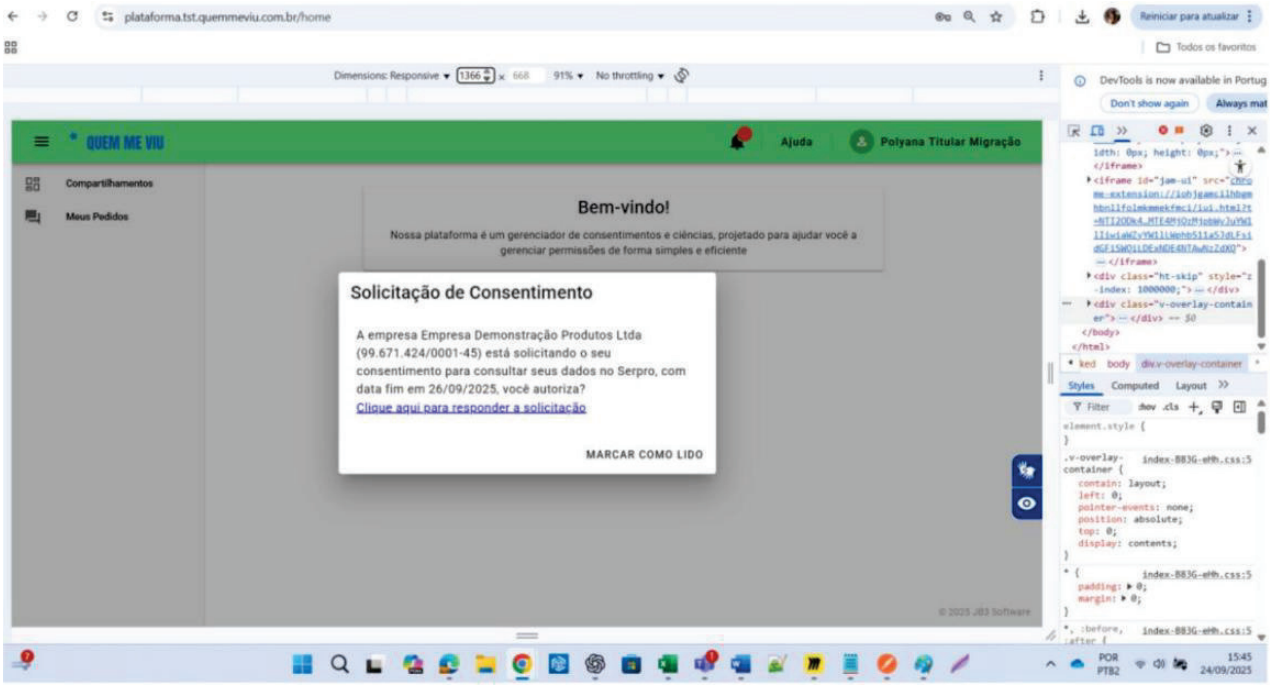
2. Responsividade

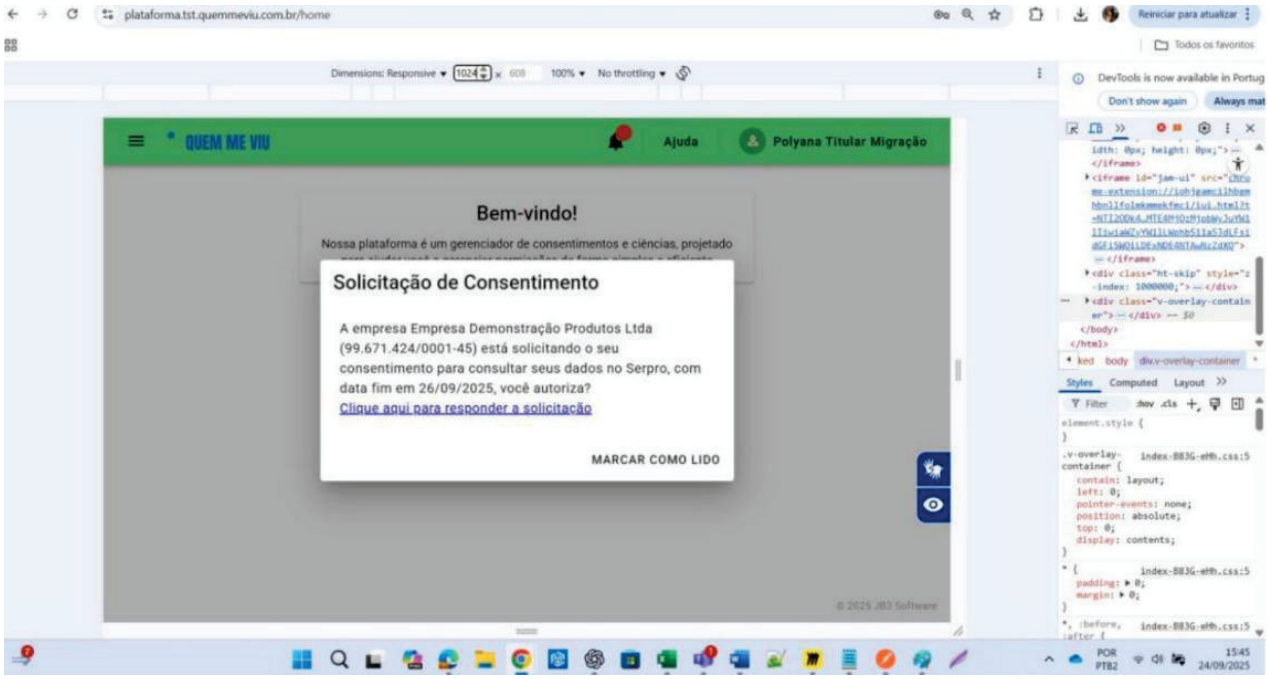
O objetivo da responsividade para desktop, smartphones e tablets visa garantir que as aplicações:
• Adapte-se automaticamente ao tamanho e orientação da tela, mantendo a legibilidade e funcionalidade em qualquer dispositivo.
• Proporcione uma experiência consistente e intuitiva, sem necessidade de zoom ou rolagem excessiva.
• Otimize a usabilidade e a estética, ajustando elementos como menus, botões, imagens e textos para diferentes resoluções.
• Melhore a acessibilidade, permitindo que usuários com diferentes dispositivos e condições de conexão tenham acesso eficiente ao conteúdo.
• Aumente a performance e engajamento, já que interfaces responsivas reduzem fricções e tornam a navegação mais agradável.

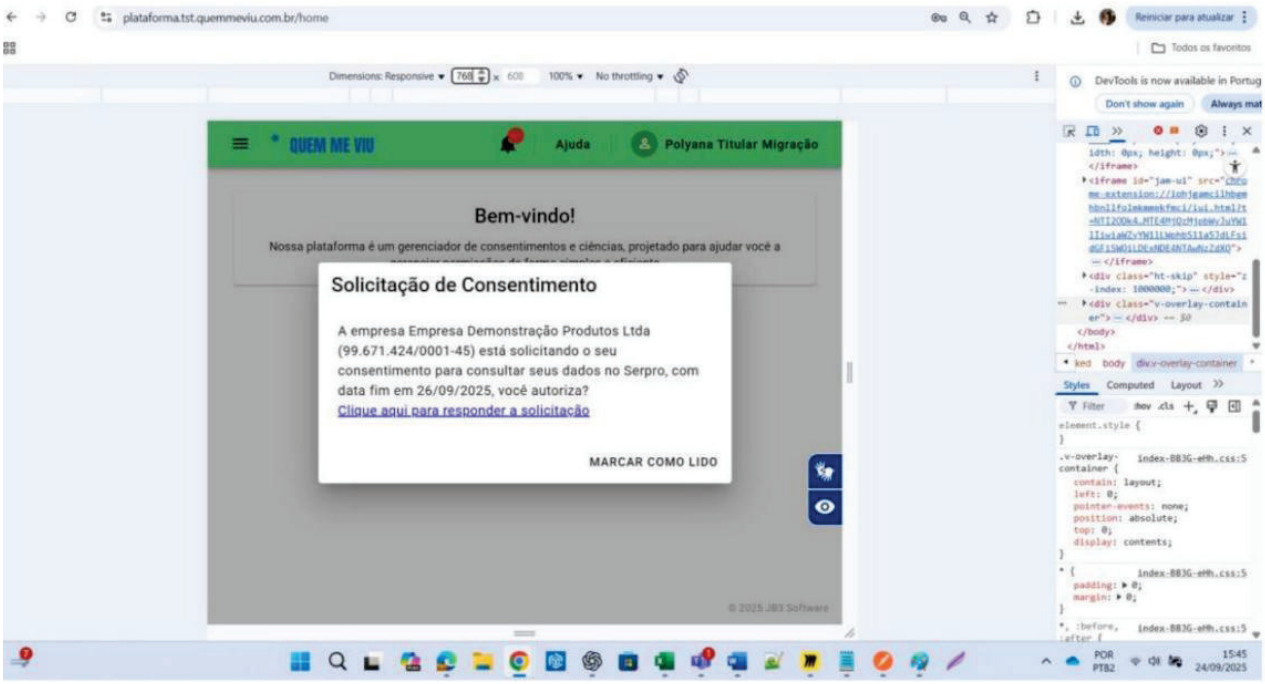
Breakpoints:
• 1440px (desktop widescreen)
• 1366px (desktop padrão)
• 1024px (tablet landscape)
• 768px (tablet portrait)
• 480px (smartphones médios)
• 320px (smartphones pequenos)

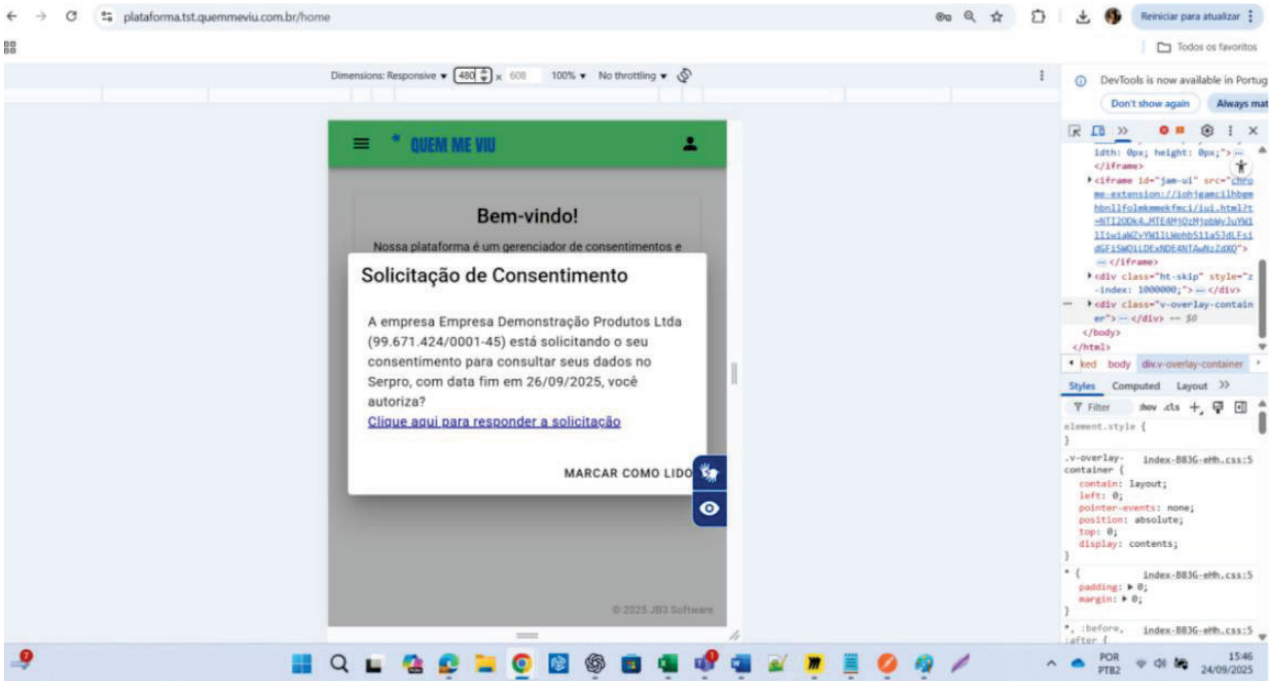

plataforma.tst.quemmeviu.com.br/titular/login
QUEM ME VIU
Insira o código enviado no seu e-mail ou sms no seu telefone.
Aguarde para reenviar o código: 47 segundos
CANCELAR
ENTRAR
Esqueceu a senha?
Ou continue com

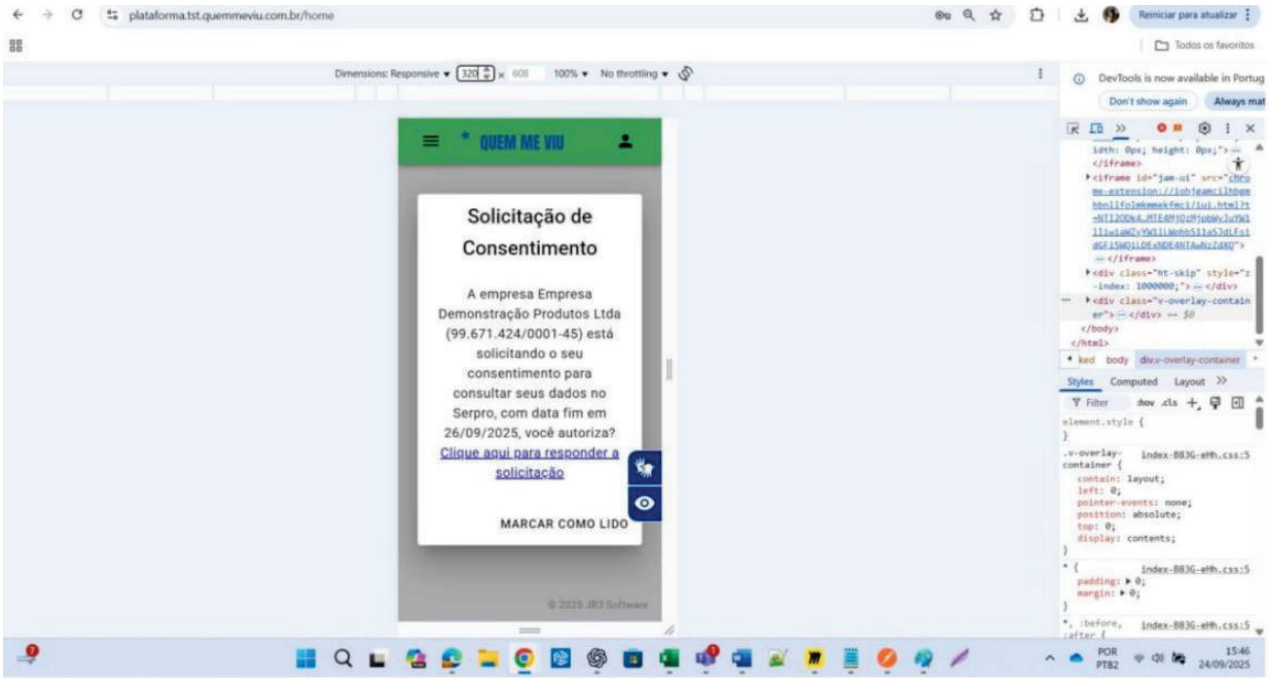

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Polyana Titular Migração
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO

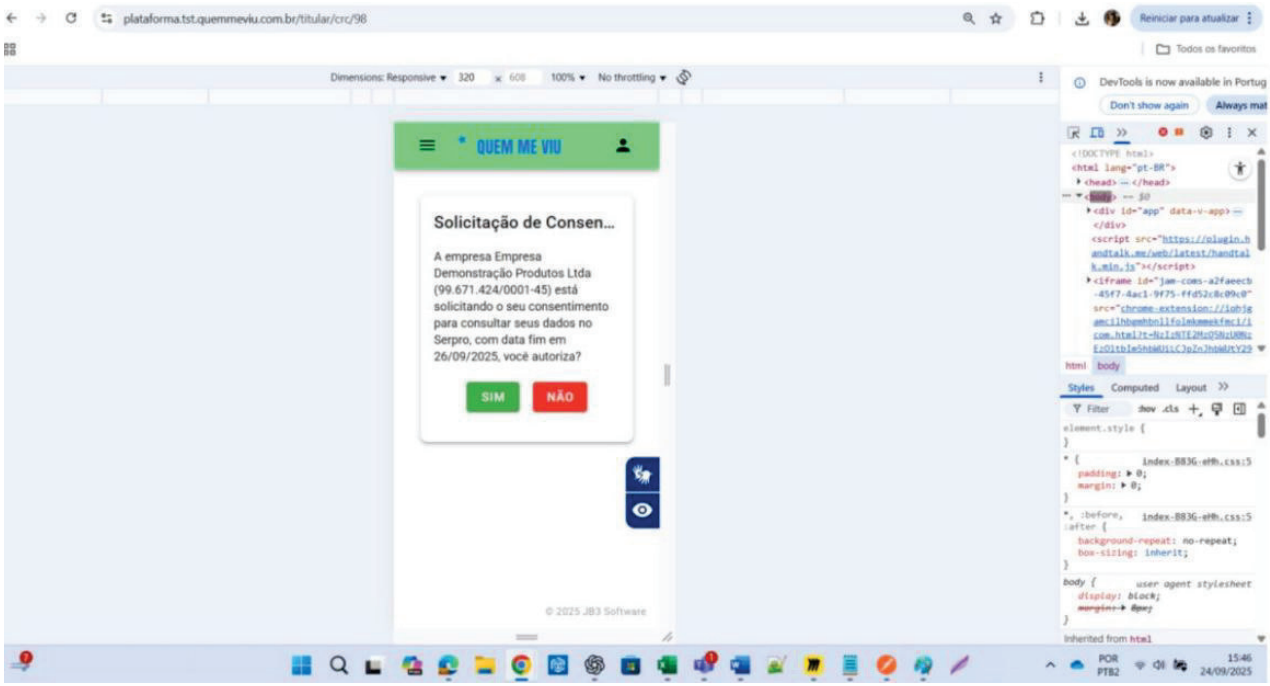

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Polyana Titular Migração
Compartilhamentos
Meus Pedidos
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO

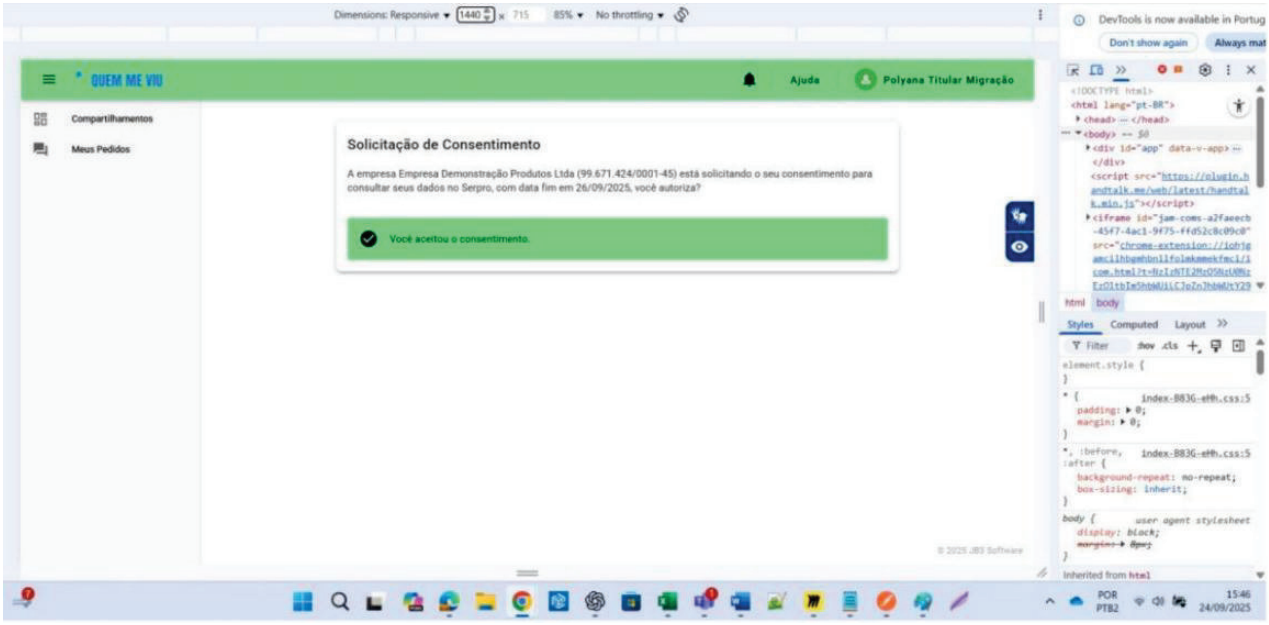

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Polyana Titular Migração
Bem-vindo!
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO

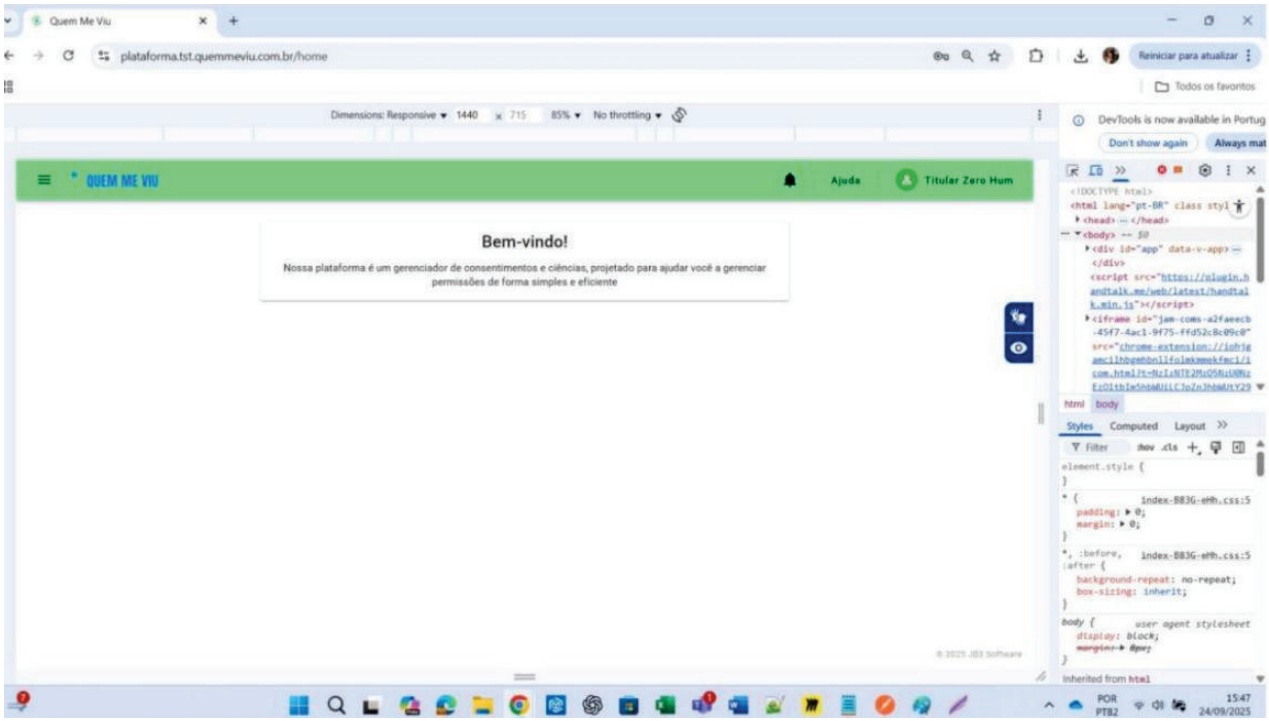

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Polyana Titular Migração
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO
© 2025 JB3 Software

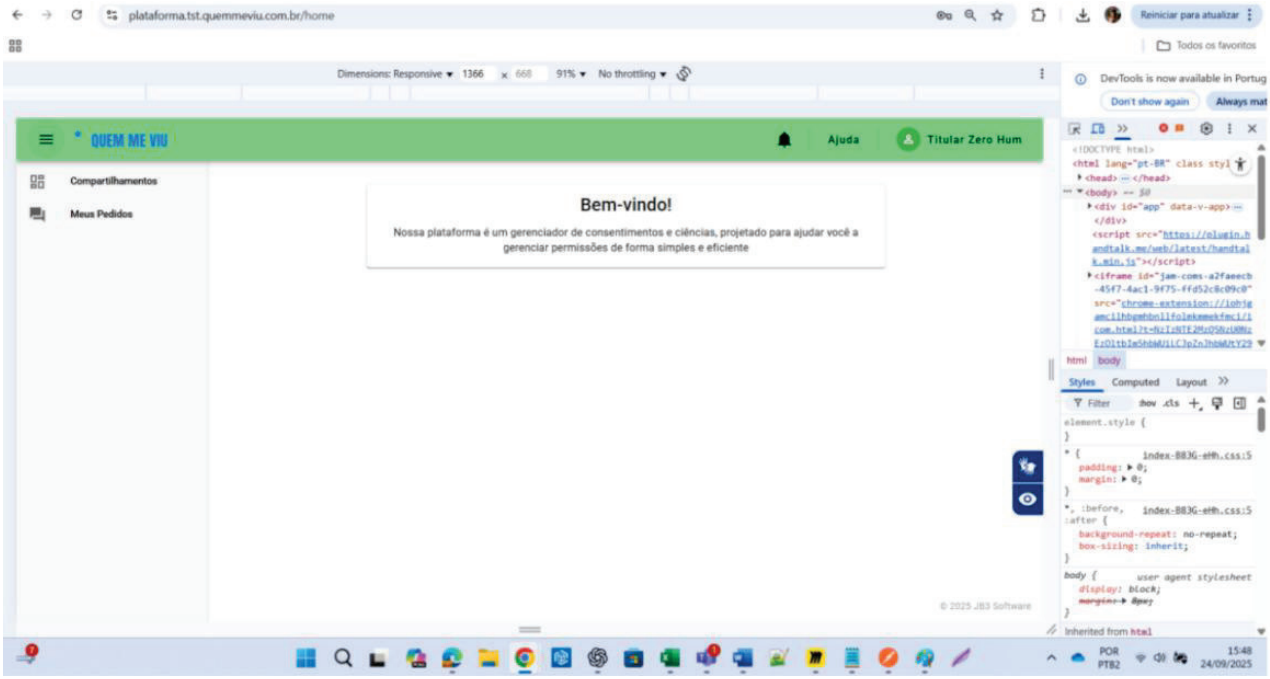

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO
© 2025 JB3 Software

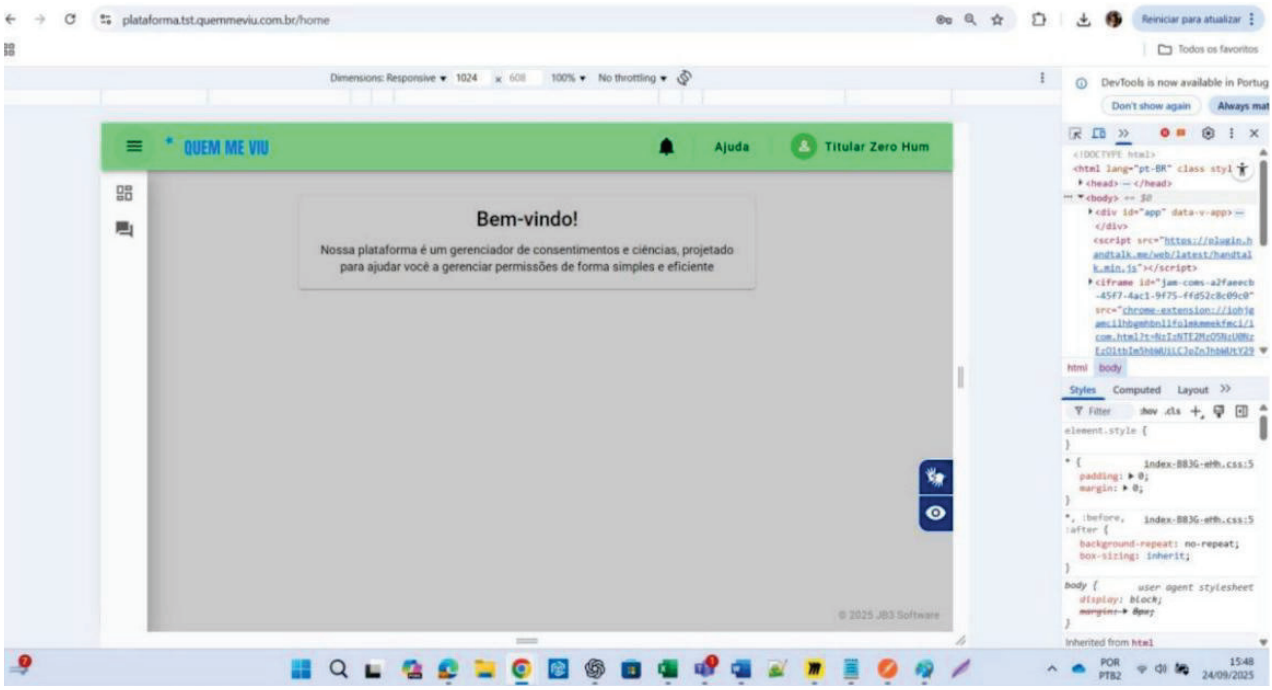

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO
© 2025 JB3 Software

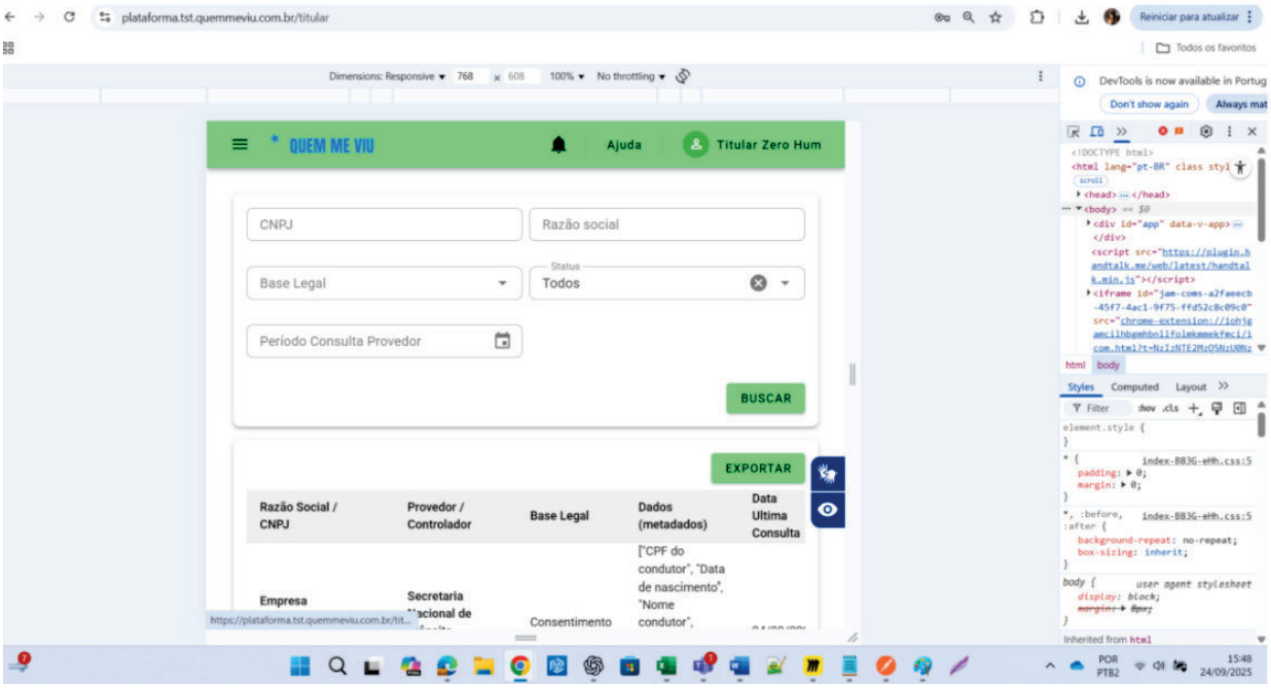

plataforma.tst.quemmeviu.com.br/titular/crc/98
QUEM ME VIU
Solicitação de Consen...
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
SIM
NÃO
© 2025 JB3 Software

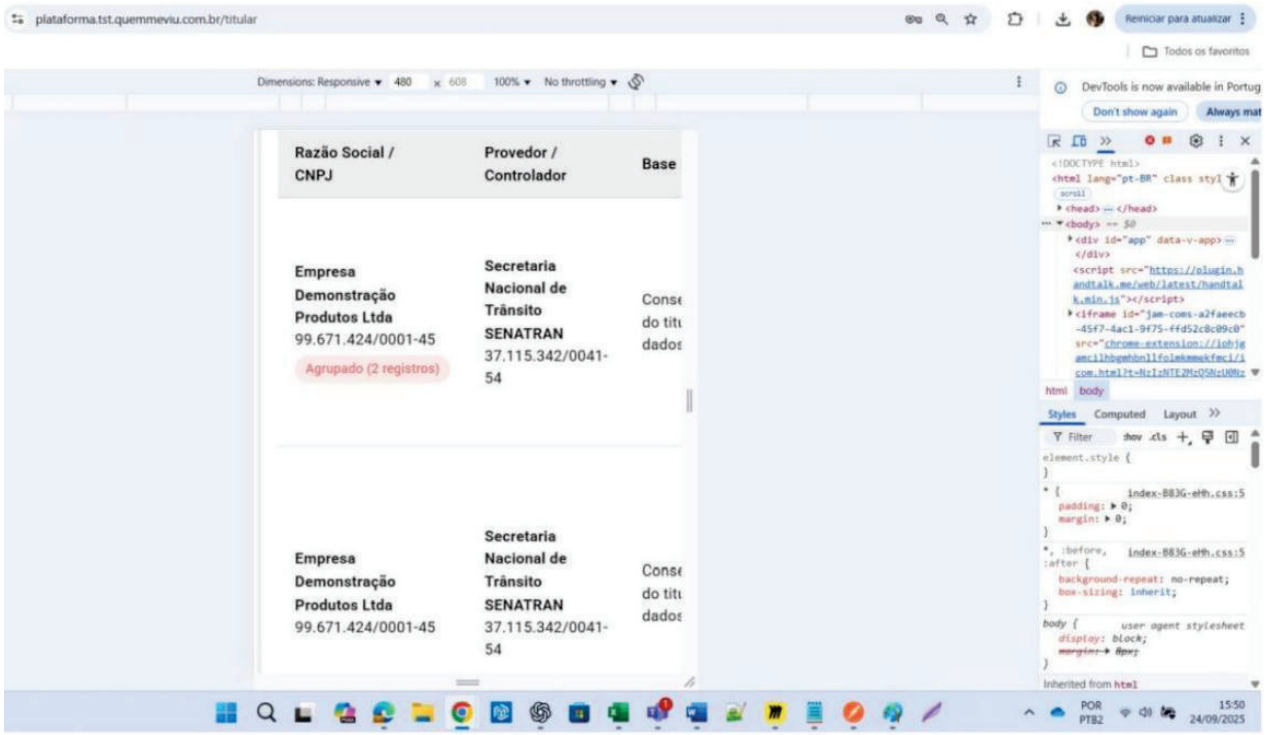

QUEM ME VIU
Ajuda
Polyana Titular Migração
Compartilhamentos
Meus Pedidos
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Você aceitou o consentimento.

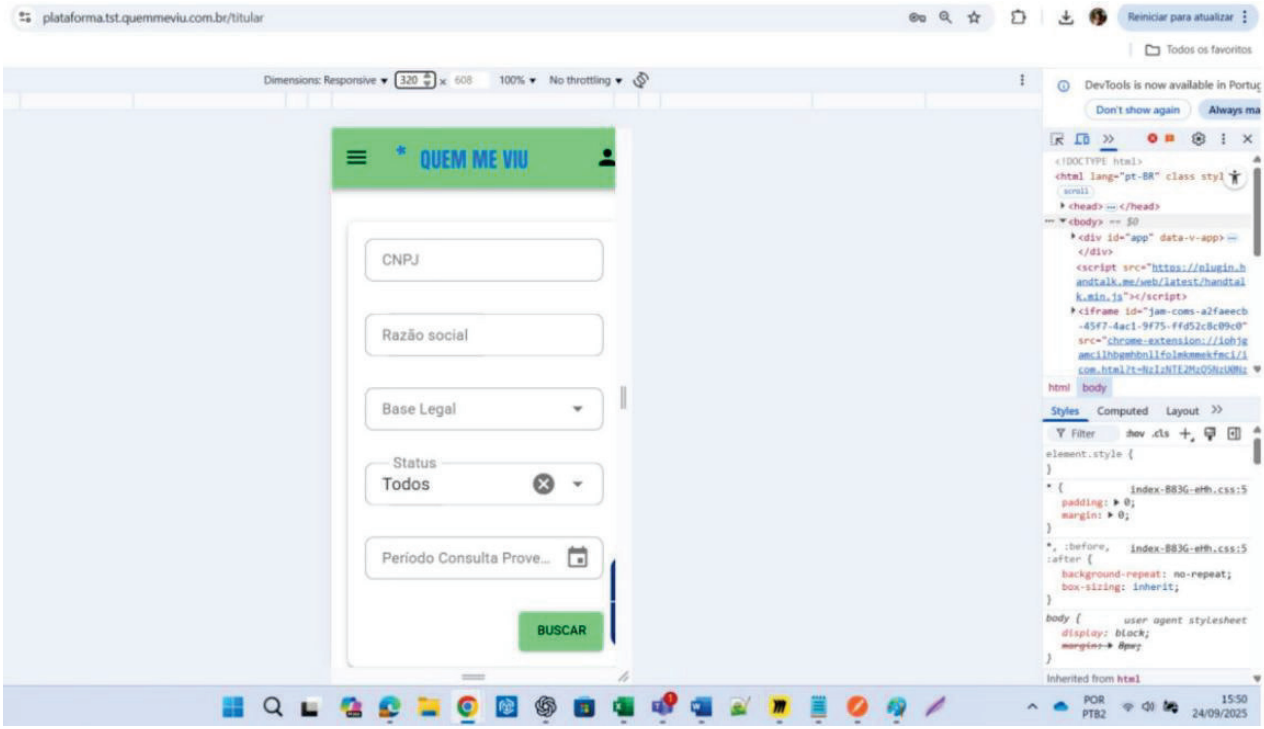

Quem Me Viu
plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Zero Hum
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente


plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Zero Hum
Compartilhamentos
Meus Pedidos
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
© 2025 JB3 Software


plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Zero Hum
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
© 2025 JB3 Software

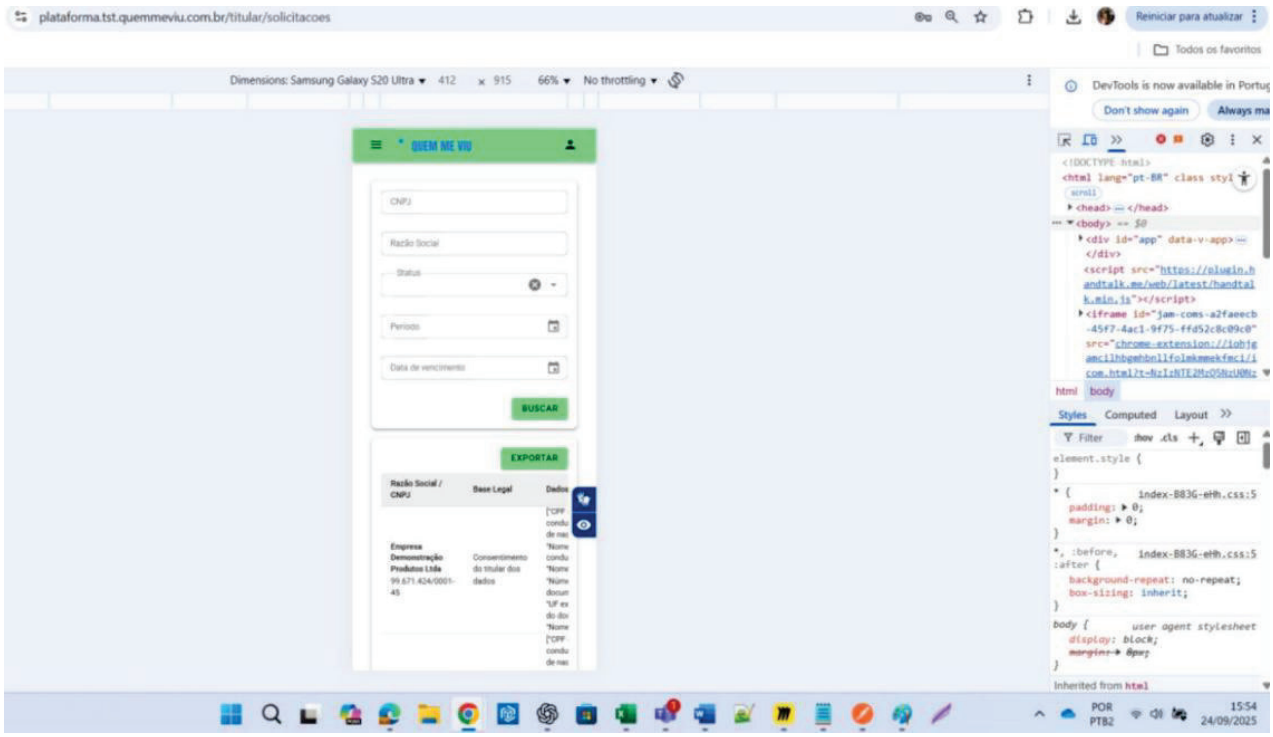

plataforma.tst.quemmeviu.com.br/titular
QUEM ME VIU
Ajuda
Titular Zero Hum
CNPJ
Razão social
Base Legal
Status
Todos
Período Consulta Provedor
BUSCAR
EXPORTAR
Razão Social / CNPJ
Provedor / Controlador
Base Legal
Dados (metadados)
Data Ultima Consulta
Empresa
Secretaria
Consentimento
["CPF do condutor", "Data de nascimento", "Nome condutor",

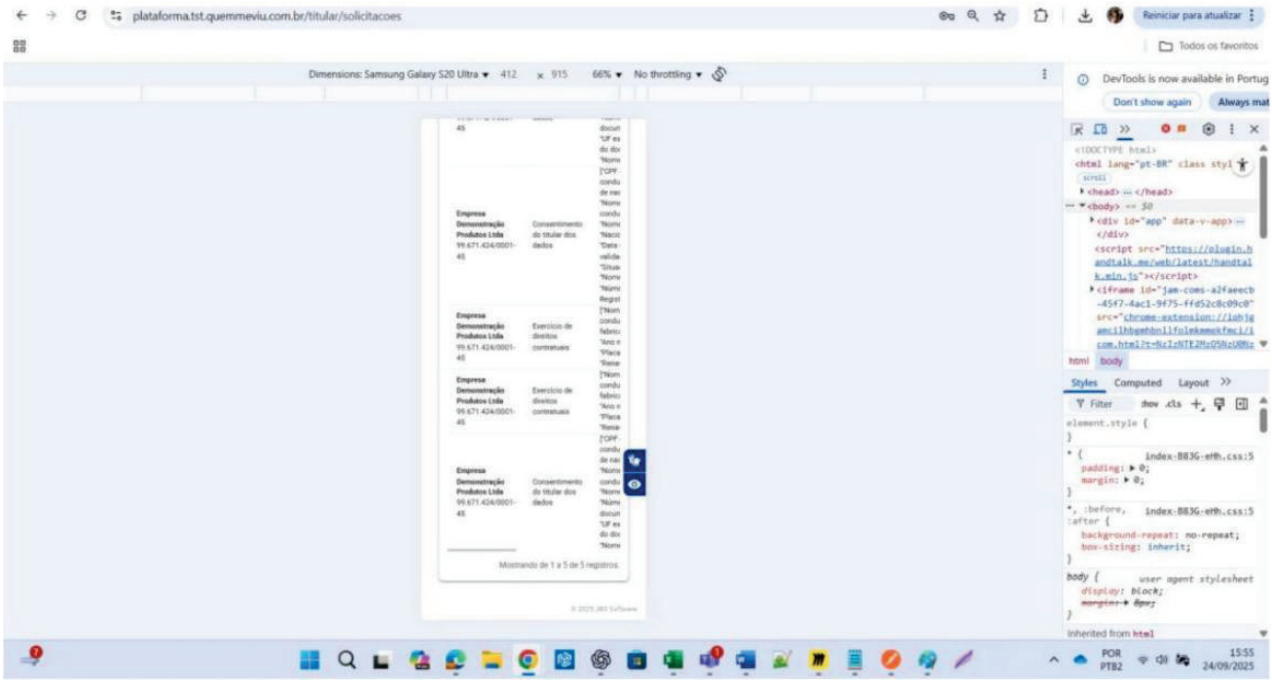

plataforma.tst.quemmeviu.com.br/titular
Razão Social / CNPJ
Provedor / Controlador
Base
Empresa Demonstração Produtos Ltda
99.671.424/0001-45
Agrupado (2 registros)
Secretaria Nacional de Trânsito SENATRAN
37.115.342/0041-54
Empresa Demonstração Produtos Ltda
99.671.424/0001-45
Secretaria Nacional de Trânsito SENATRAN
37.115.342/0041-54

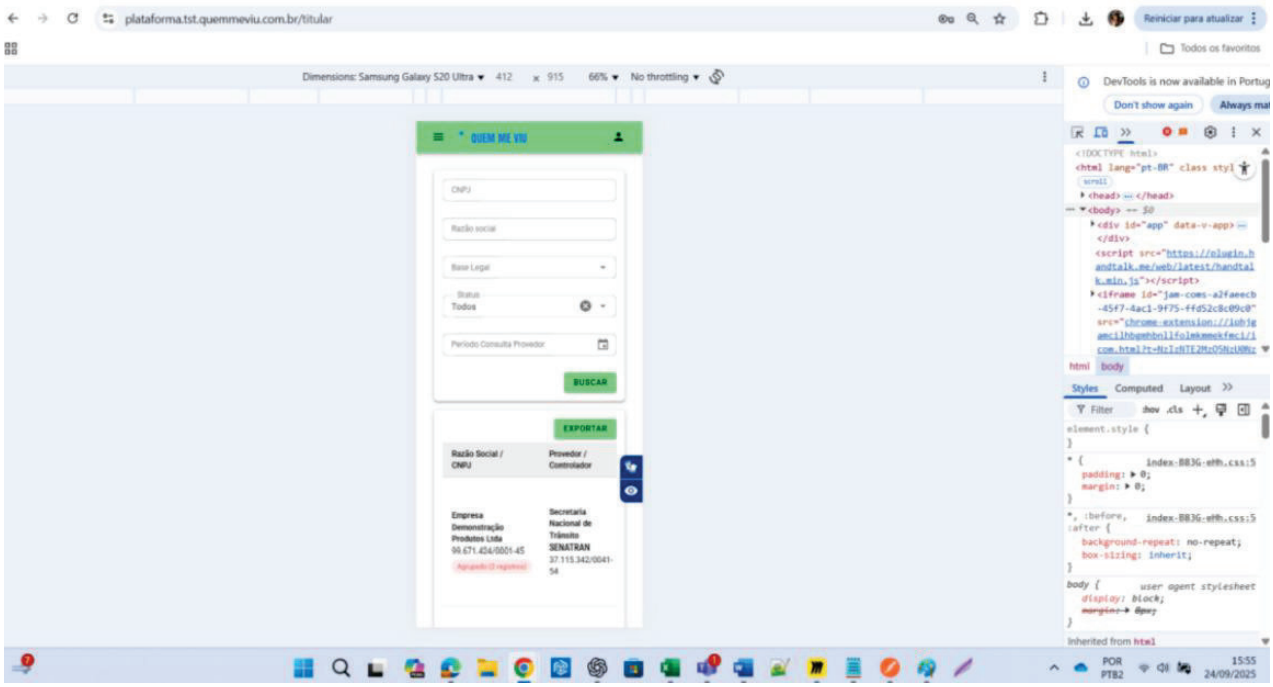


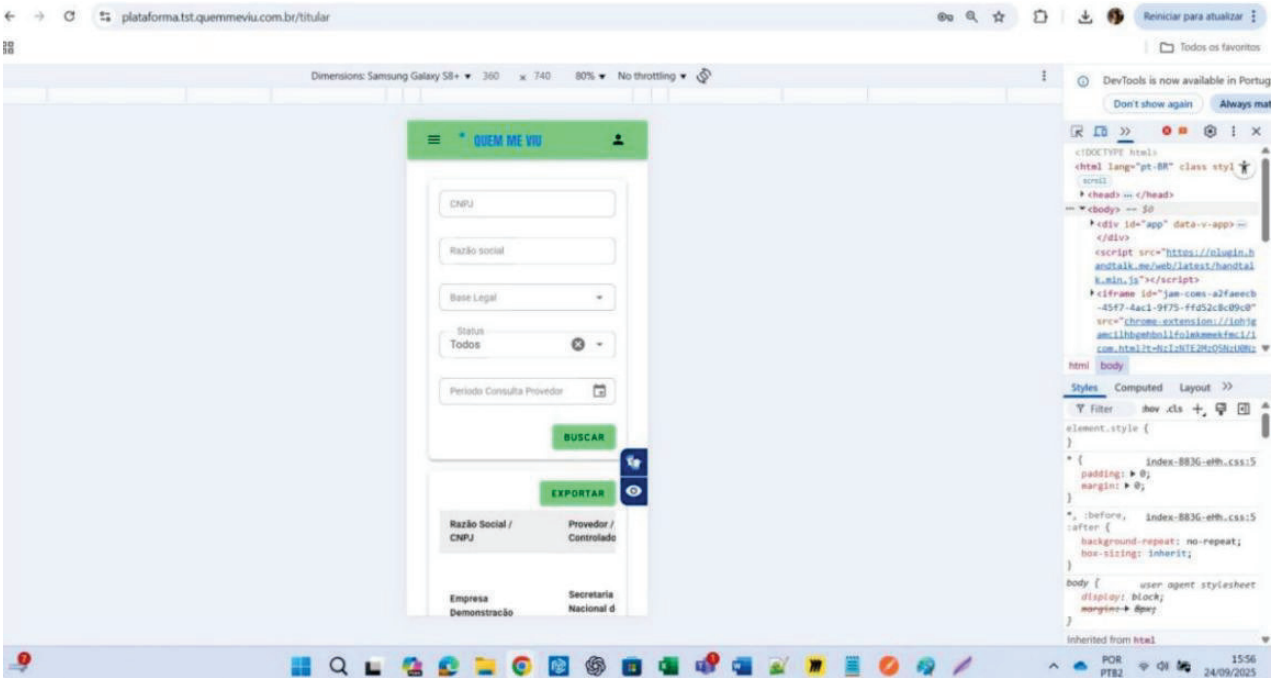
Smartphone

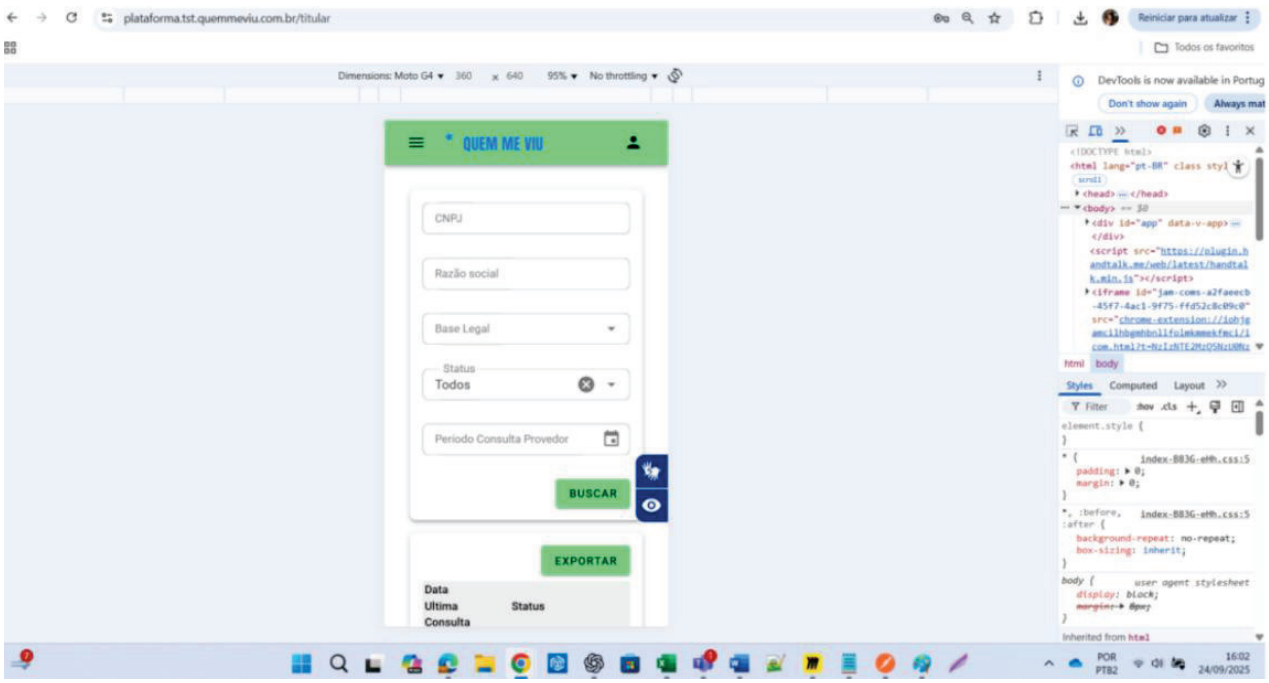
Android

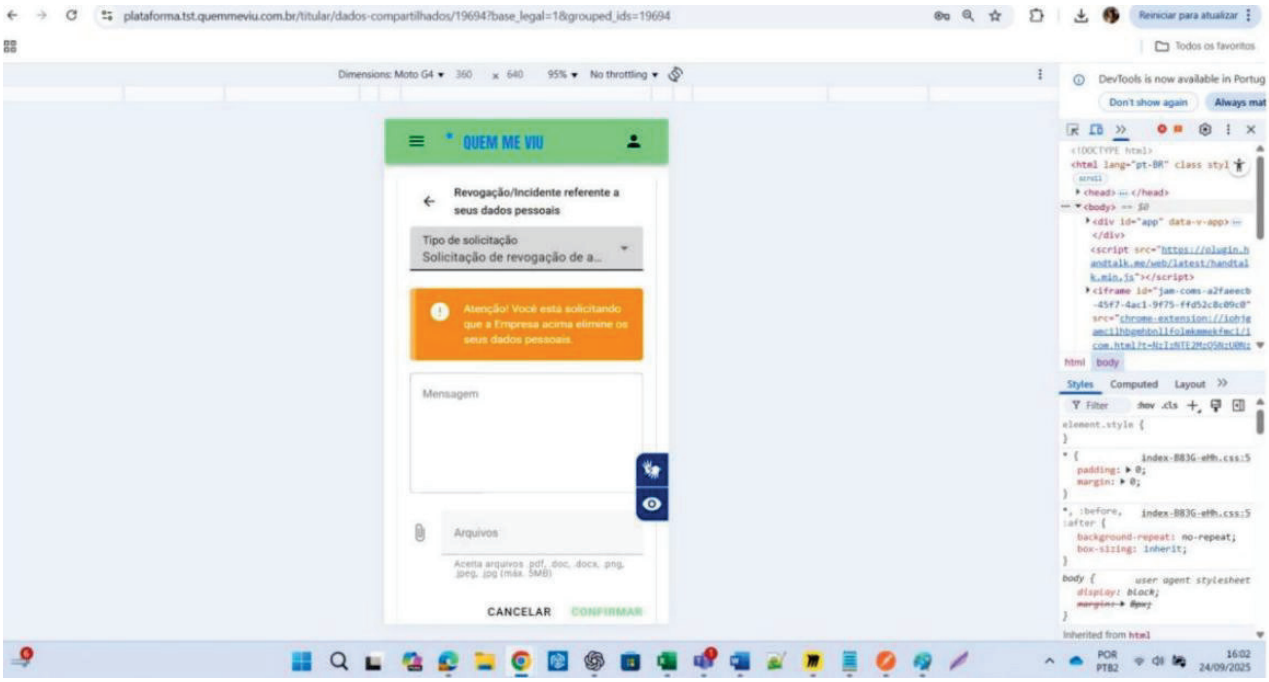



plataforma.tst.quemmeviu.com.br/titular/solicitacoes
Dimensions: Samsung Galaxy S20 Ultra 412 x 915 66% No throttling
Mostrando de 1 a 5 de 5 registros.

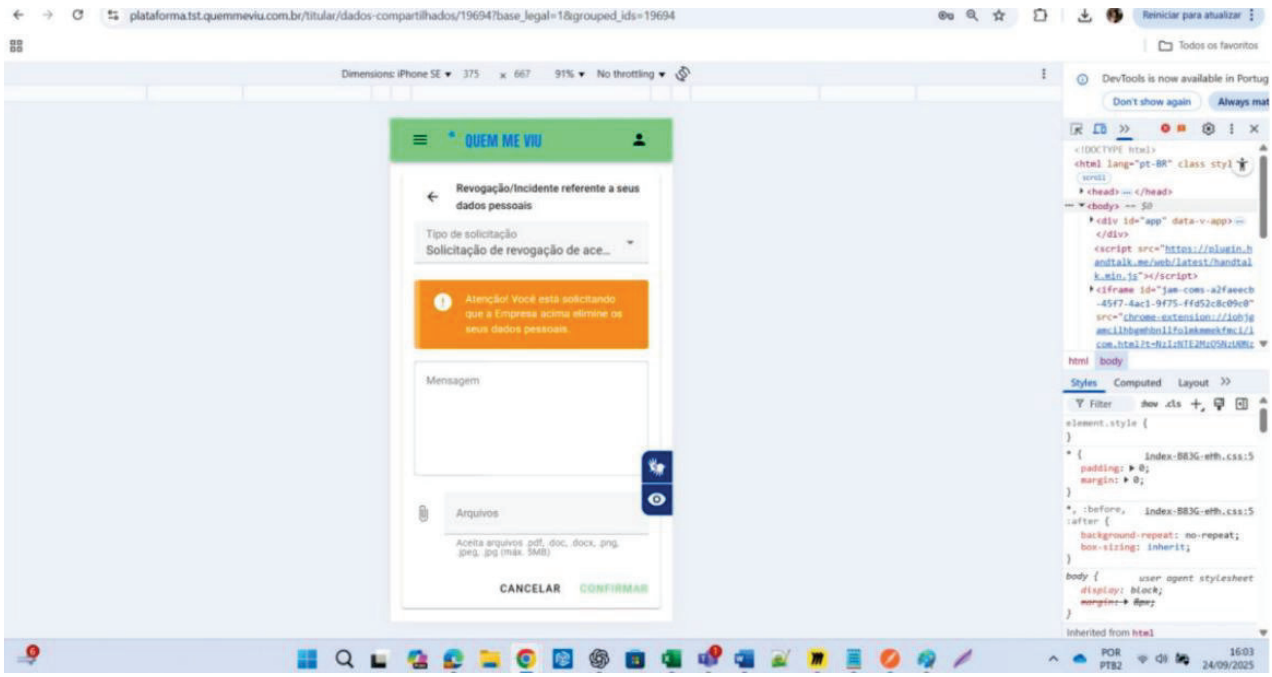

plataforma.tst.quemmeviu.com.br/titular
Dimensions: Samsung Galaxy S20 Ultra 412 x 915 66% No throttling
QUEM ME VIU
CNPJ
Razão social
Base Legal
Status
Todos
Período Consulta Provedor
BUSCAR
EXPORTAR
Razão Social / CNPJ
Provedor / Controlador
Empresa Demonstração Produtos Ltda 99.671.424/0001-45
Secretaria Nacional de Trânsito SENATRAN 37.115.342/0041-54

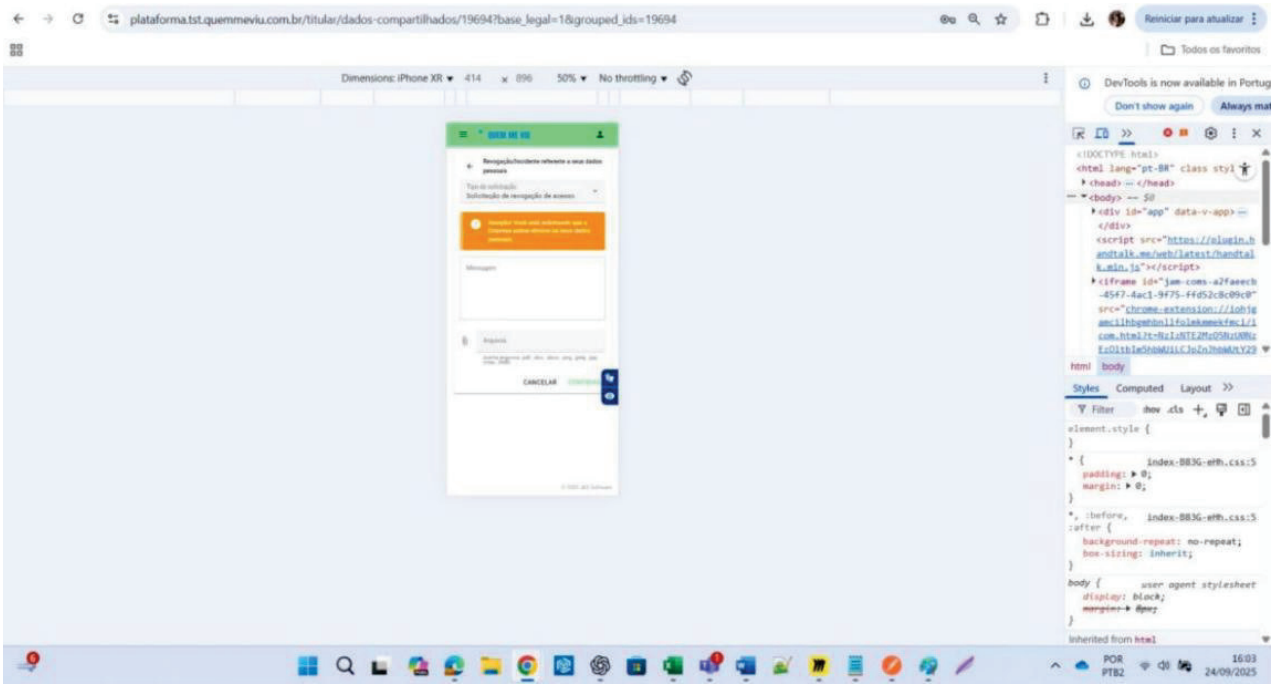

plataforma.tst.quemmeviu.com.br/titular
Reiniciar para atualizar
Dimensions: Samsung Galaxy S8+ 360 x 740 80% No throttling
QUEM ME VIU
CNPJ
Razão social
Base Legal
Status
Todos
Periodo Consulta Provedor
BUSCAR
EXPORTAR
Razão Social / CNPJ
Provedor / Controlado
Empresa Demonstração
Secretaria Nacional d
DevTools is now available in Portug
Don't show again
Always mat
Styles
Computed
Layout
Filter
element.style {
}
* {
padding: ▶ 0;
margin: ▶ 0;
}
*, :before, :after {
background-repeat: no-repeat;
box-sizing: inherit;
}
body {
display: block;
}
Inherited from html
POR PTB2
15:56
24/09/2025

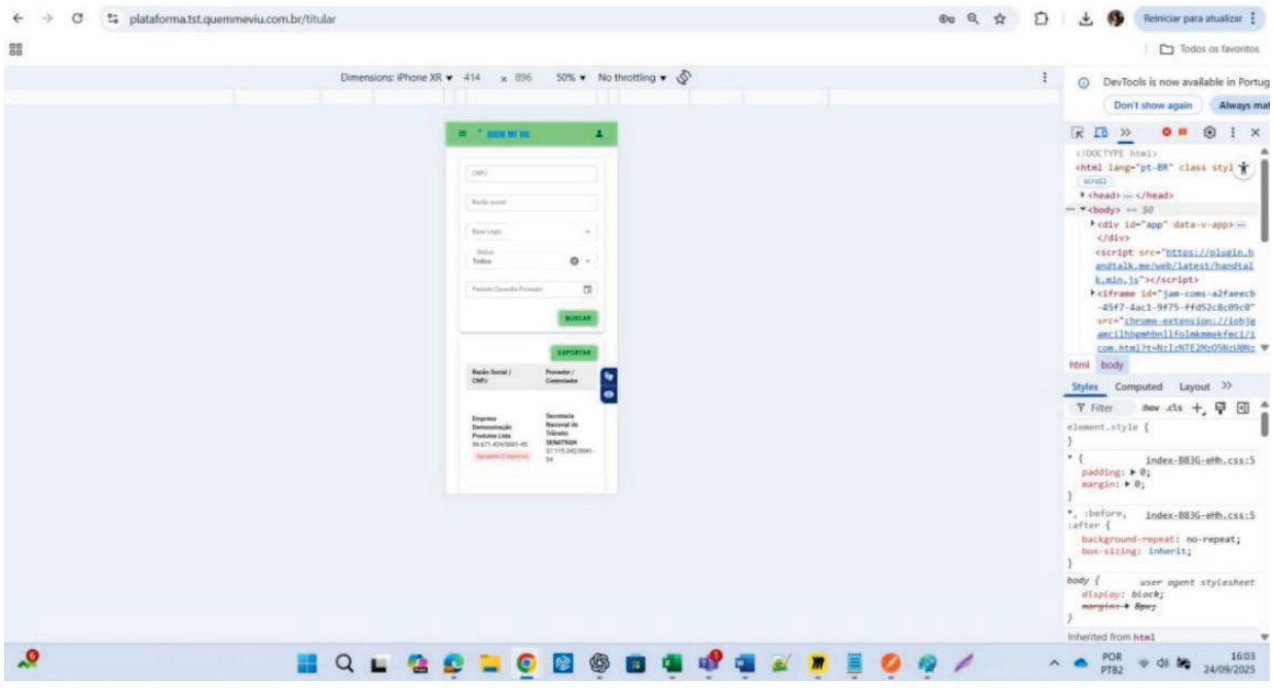

plataforma.tst.quemmeviu.com.br/titular
Reiniciar para atualizar
Dimensions: Moto G4 360 x 640 95% No throttling
QUEM ME VIU
CNPJ
Razão social
Base Legal
Status
Todos
Periodo Consulta Provedor
BUSCAR
EXPORTAR
Data Ultima Consulta
Status
DevTools is now available in Portug
Don't show again
Always mat
Styles
Computed
Layout
Filter
element.style {
}
* {
padding: ▶ 0;
margin: ▶ 0;
}
*, :before, :after {
background-repeat: no-repeat;
box-sizing: inherit;
}
body {
display: block;
}
Inherited from html
POR PTB2
16:02
24/09/2025

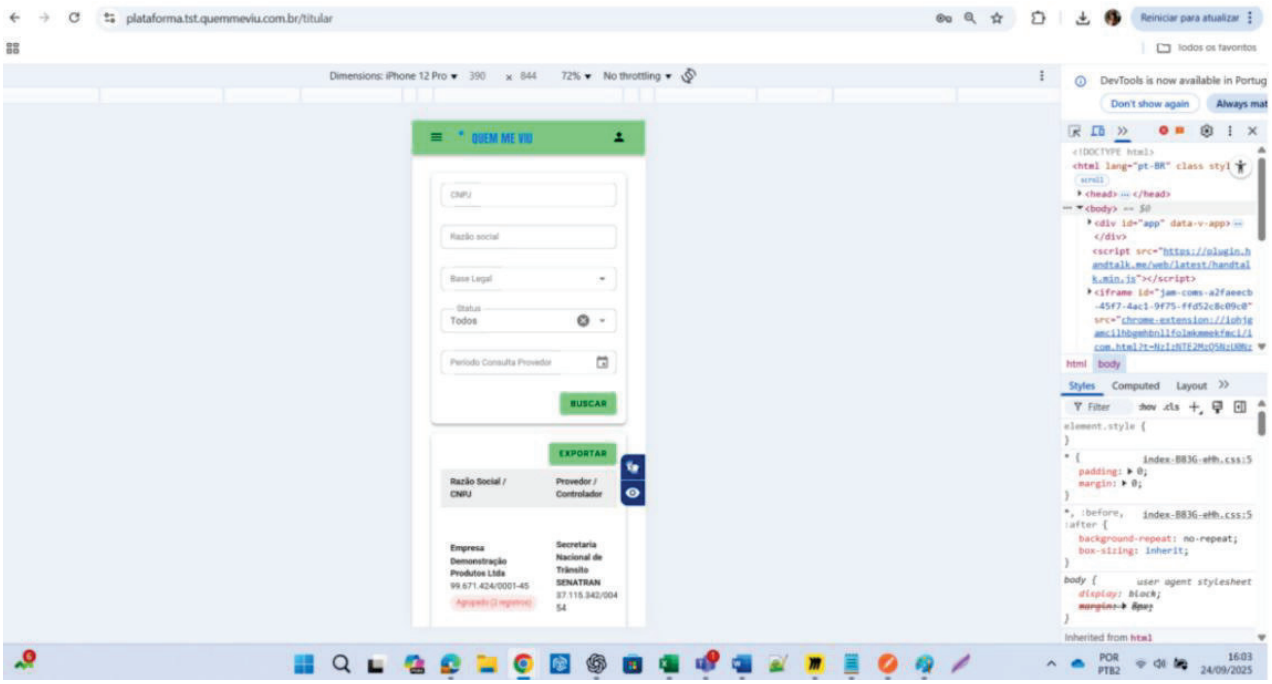

QUEM ME VIU
Revogação/Incidente referente a seus dados pessoais
Tipo de solicitação
Solicitação de revogação de a...
Atenção! Você está solicitando que a Empresa acima elimine os seus dados pessoais.
Mensagem
Arquivos
CANCELAR
CONFIRMAR

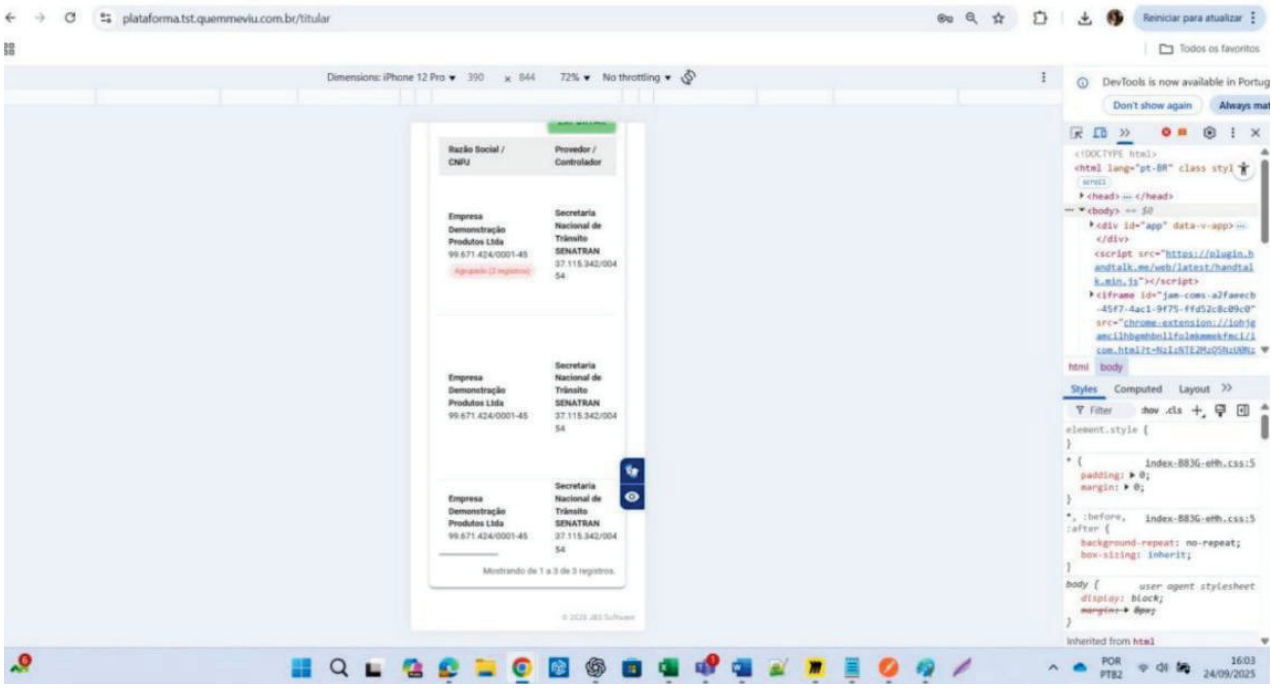
IOS


QUEM ME VIU
Revogação/Incidente referente a seus dados pessoais
Tipo de solicitação
Solicitação de revogação de ace...
Atenção! Você está solicitando que a Empresa acima elimine os seus dados pessoais.
Mensagem
Arquivos
CANCELAR
CONFIRMAR

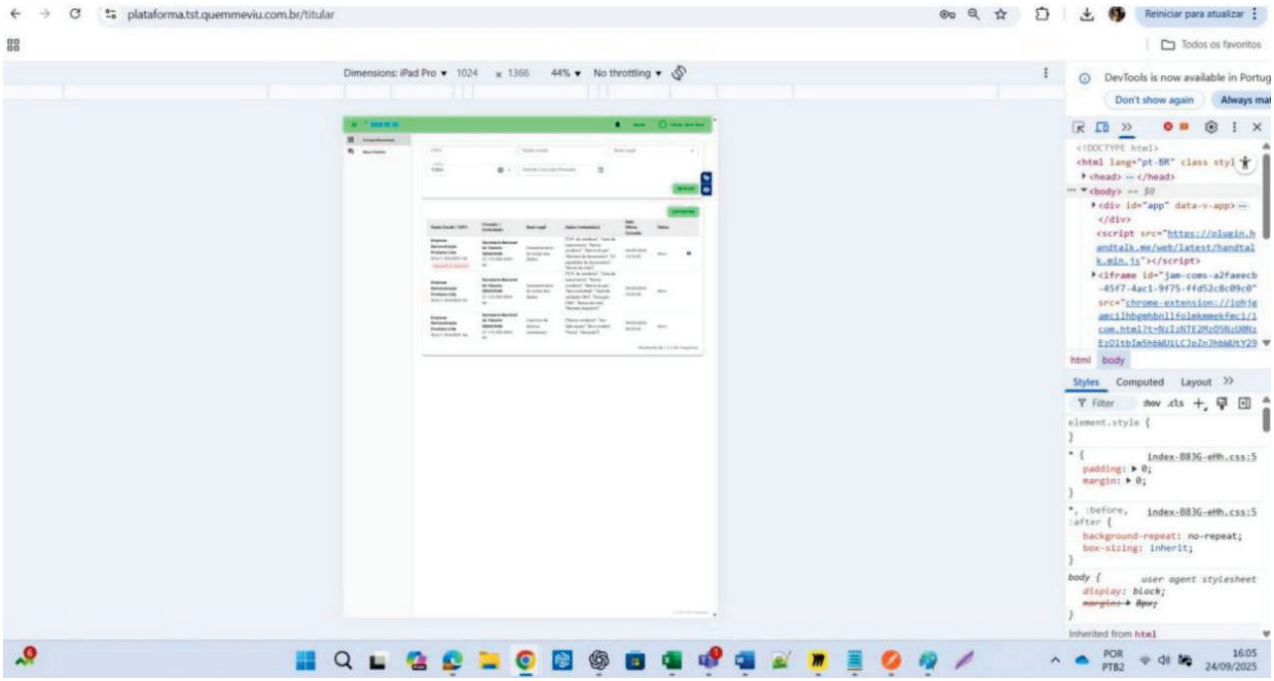

plataforma.tst.quemmeviu.com.br/titular/dados-compartilhados/19694?base_legal=1&grouped_ids=19694
Reiniciar para atualizar
Dimensions: iPhone XR 414 x 896 50% No throttling
DevTools is now available in Portug
Don't show again
CANCELAR
Styles
Computed
Layout
POR PTB2
16:03 24/09/2025

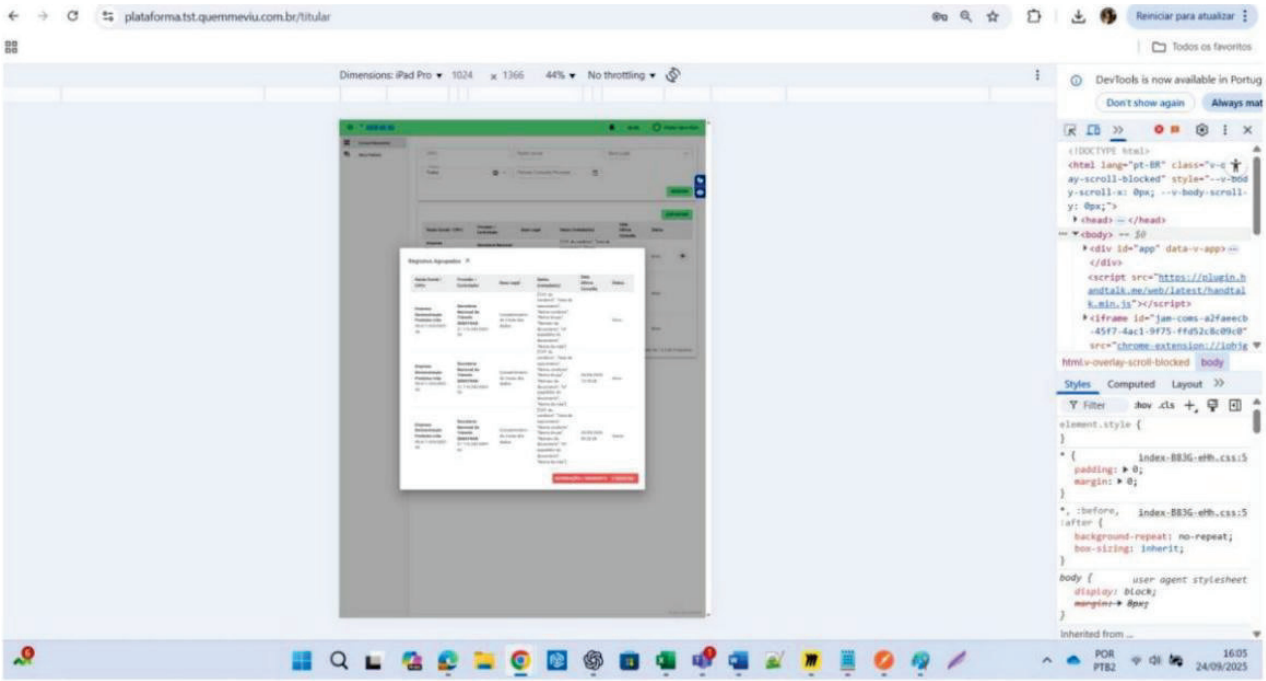

plataforma.tst.quemmeviu.com.br/titular
Reiniciar para atualizar
Dimensions: iPhone XR 414 x 896 50% No throttling
DevTools is now available in Portug
Don't show again
BUSCAR
EXPORTAR
Styles
Computed
Layout
POR PTB2
16:03 24/09/2025

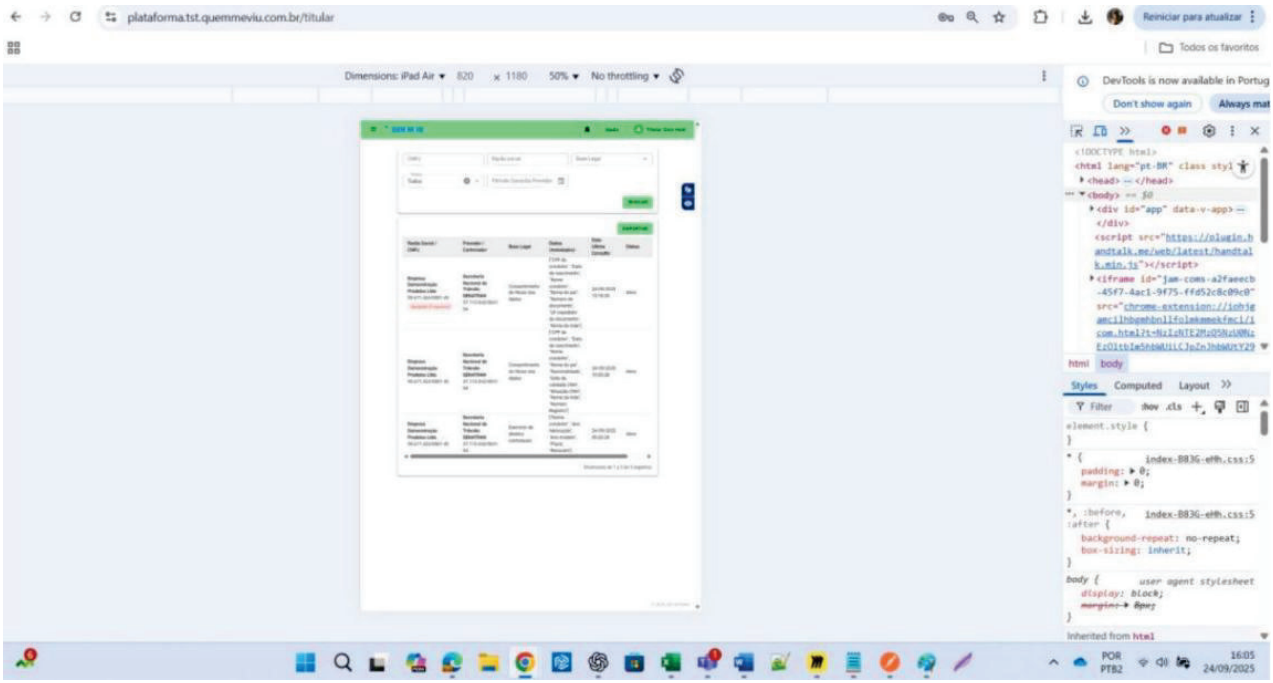

plataforma.tst.quemmeviu.com.br/titular
QUEM ME VIU
CNPJ
Razão social
Base Legal
Status
Todos
Período Consulta Provedor
BUSCAR
EXPORTAR
Razão Social / CNPJ
Provedor / Controlador
Empresa Demonstração Produtos Ltda
99.671.424/0001-45
Secretaria Nacional de Trânsito SENATRAN
37.115.342/0054

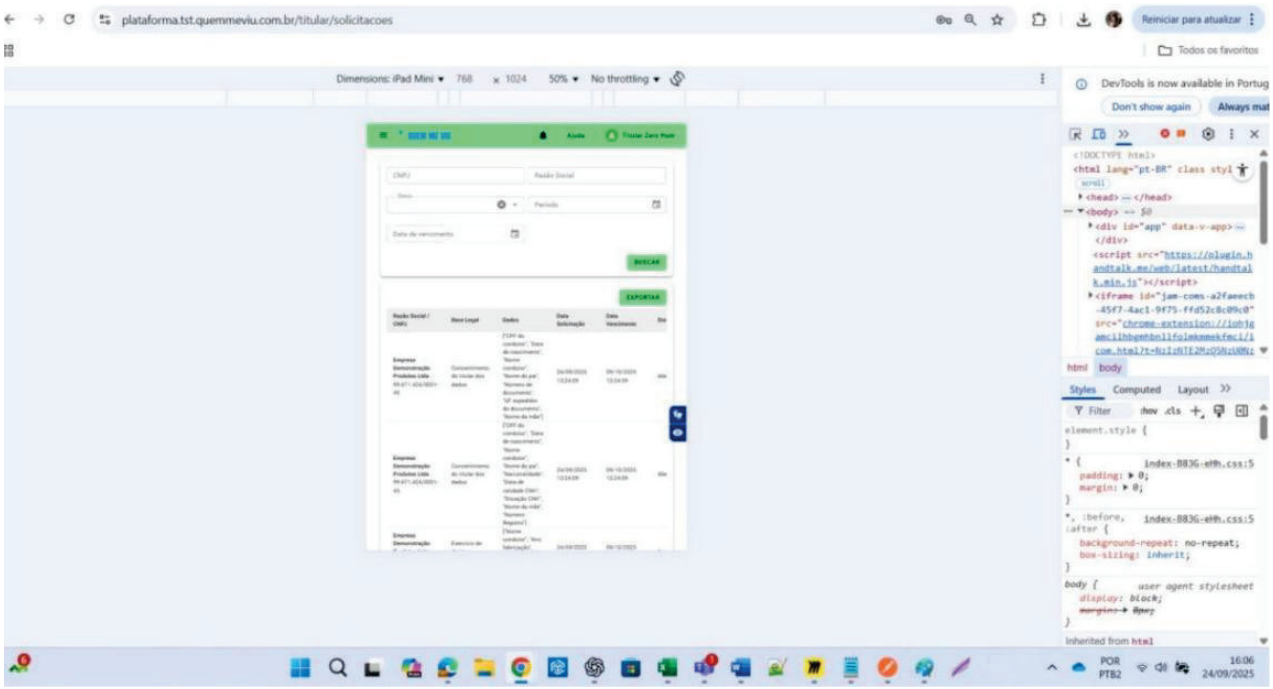

plataforma.tst.quemmeviu.com.br/titular
Razão Social / CNPJ
Provedor / Controlador
Empresa Demonstração Produtos Ltda
99.671.424/0001-45
Secretaria Nacional de Trânsito SENATRAN
37.115.342/0054
Mostrando de 1 a 3 de 3 registros.

Tablet


plataforma.tst.quemmeviu.com.br/titular
Reiniciar para atualizar
Dimensions: iPad Pro 1024 x 1366 44% No throttling
DevTools is now available in Portug
Don't show again
Always mat
Styles
Computed
Layout
element.style {
}
* {
padding: 0;
margin: 0;
}
body {
display: block;
}
POR
PTB2
16:05
24/09/2025


plataforma.tst.quemmeviu.com.br/titular
Reiniciar para atualizar
Dimensions: iPad Pro 1024 x 1366 44% No throttling
DevTools is now available in Portug
Don't show again
Always mat
Styles
Computed
Layout
element.style {
}
* {
padding: 0;
margin: 0;
}
body {
display: block;
}
POR
PTB2
16:05
24/09/2025



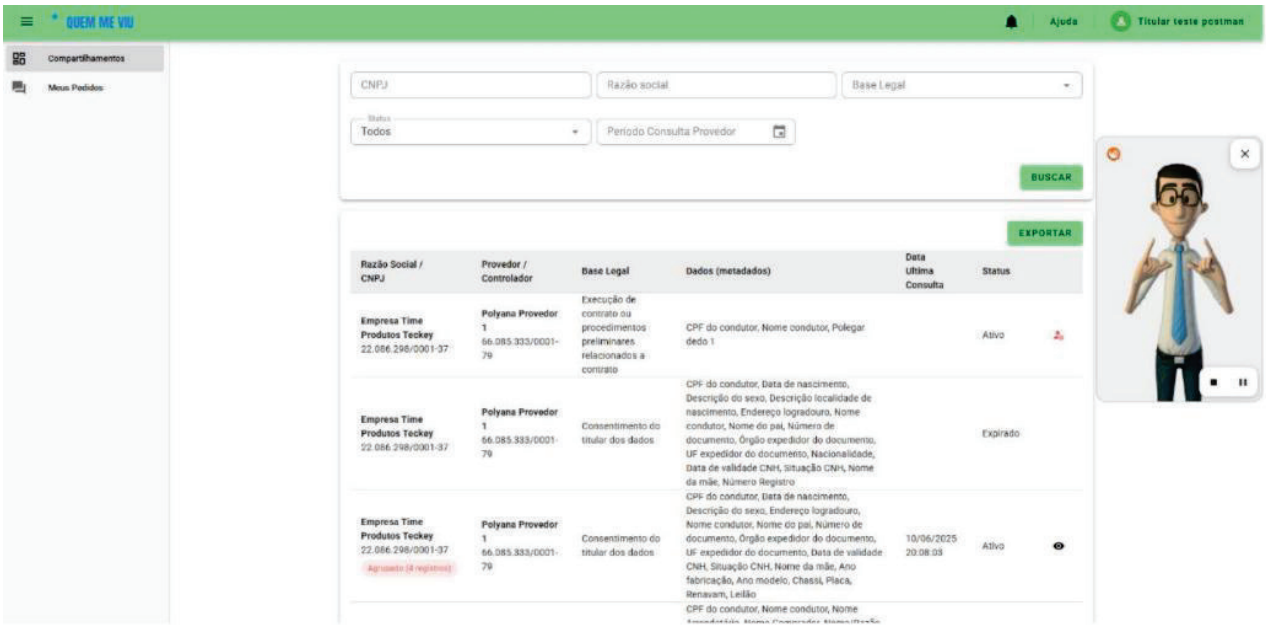


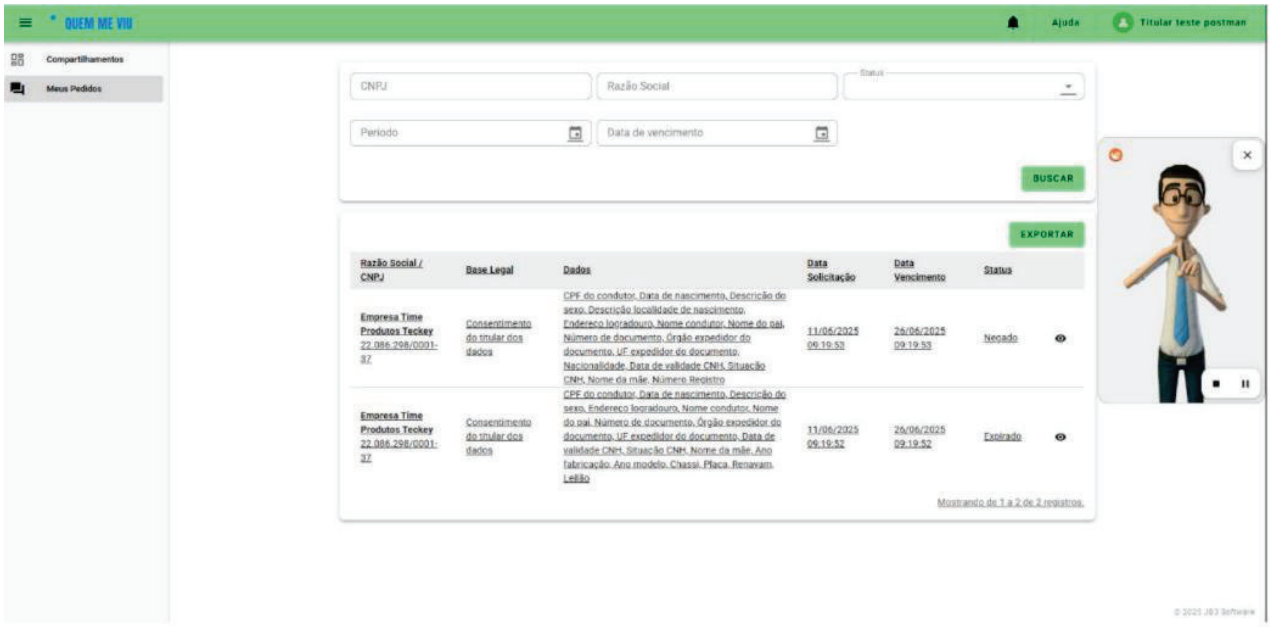
3. Acessibilidade

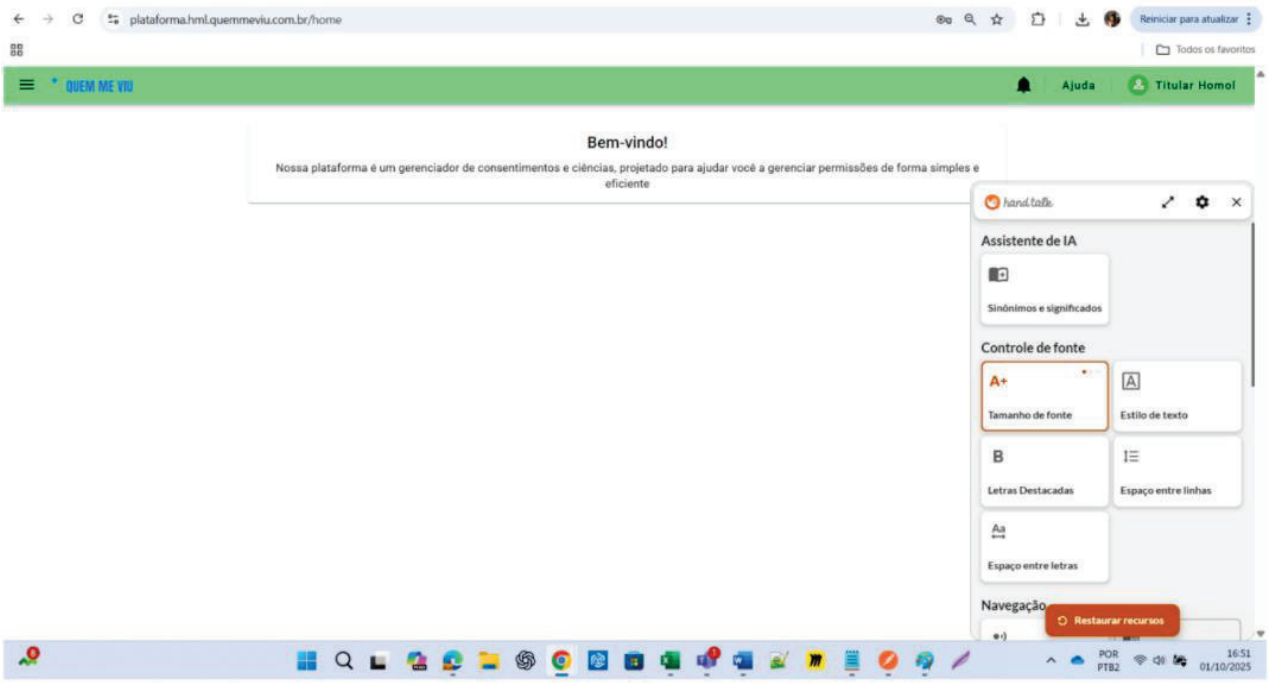
A importância de garantir acessibilidade nas aplicações da GCC está diretamente ligada à inclusão e à conformidade com padrões globais. Aqui estão os principais pontos:

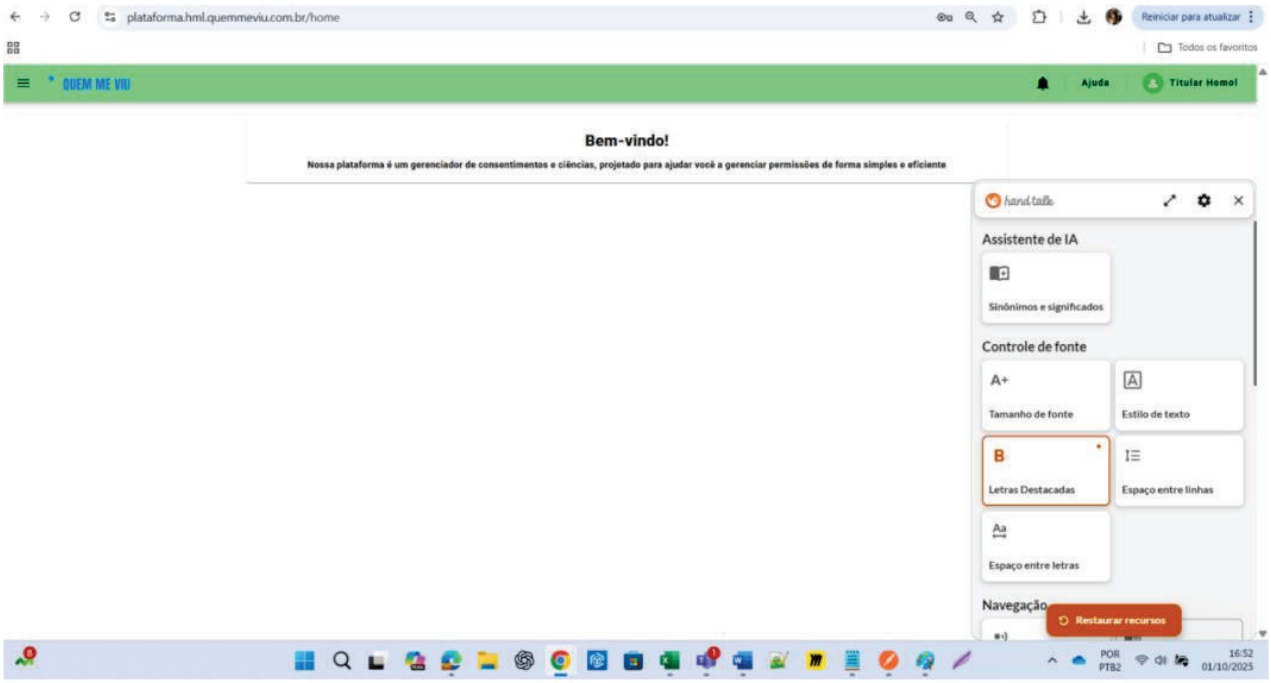
• Inclusão Digital: Permite que pessoas com deficiência visual, auditiva, motora ou cognitiva utilizem as aplicações sem barreiras, garantindo igualdade de acesso à informação e serviços.

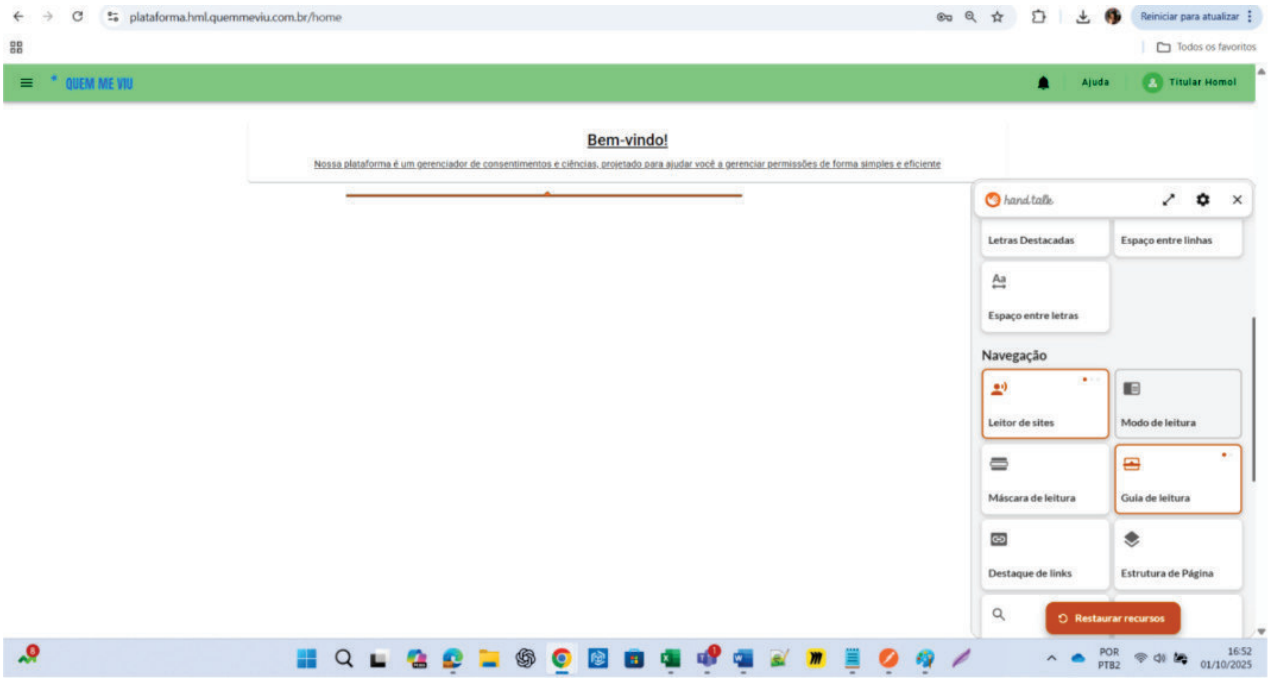
• Conformidade com Normas: Atender às diretrizes da WCAG 2.1 e legislações como a Lei Brasileira de Inclusão (LBI) evita riscos legais e demonstra compromisso com boas práticas.
• Melhoria da Experiência do Usuário: Interfaces acessíveis são mais claras, intuitivas e funcionais para todos os usuários, não apenas para pessoas com deficiência.
• Responsabilidade Social e Reputação: Empresas que priorizam acessibilidade reforçam sua imagem como organizações éticas e comprometidas com diversidade e inclusão.
• Aumento do Alcance: Aplicações acessíveis atingem um público maior, incluindo milhões de pessoas com algum tipo de deficiência, ampliando engajamento e oportunidades de negócio.
Na JB3 utilizamos o plugin da Hand Talk https://www.handtalk.me/br/ , o mais inovador ecossistema de acessibilidade digital. A pessoa usuária poderá acessar o tradutor de sites (língua de sinais) e utilizar uma série de recursos assistidos como controle de fonte, estilo de texto, letras destacadas, espaços entre linhas, espaço entre letras, leitor de sites, modo de leitura, máscara de leitura, guia de leitura, destaque de links, estrutura de página, lupa de conteúdo, esconder imagens, destacar cabeçalho, pausar animações, parar sons, controle de cor, entre outros.

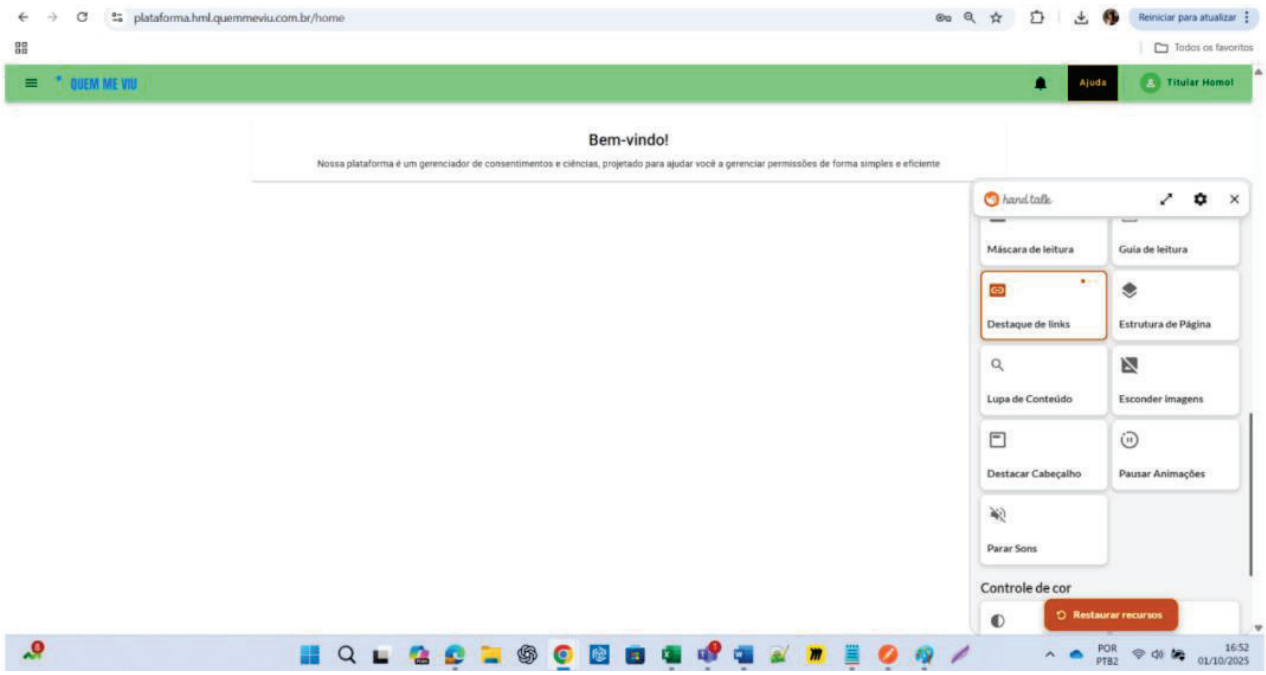

QUEM ME VIU
Ajuda
Titular teste postman
Compartilhamentos
Meus Pedidos
CNPJ
Razão social
Base Legal
Status
Todos
Período Consulta Provedor
BUSCAR
EXPORTAR
Razão Social / CNPJ
Provedor / Controlador
Base Legal
Dados (metadados)
Data Ultima Consulta
Status
Empresa Time Produtos Teckey 22.086.298/0001-37
Polyana Provedor 1 66.085.333/0001-79
Execução de contrato ou procedimentos preliminares relacionados a contrato
CPF do condutor, Nome condutor, Polegar dedo 1
Ativo
Consentimento do titular dos dados
CPF do condutor, Data de nascimento, Descrição do sexo, Descrição localidade de nascimento, Endereço logradouro, Nome condutor, Nome do pai, Número de documento, Órgão expedidor do documento, UF expedidor do documento, Nacionalidade, Data de validade CNH, Situação CNH, Nome da mãe, Número Registro
Expirado
CPF do condutor, Data de nascimento, Descrição do sexo, Endereço logradouro, Nome condutor, Nome do pai, Número de documento, Órgão expedidor do documento, UF expedidor do documento, Data de validade CNH, Situação CNH, Nome da mãe, Ano fabricação, Ano modelo, Chassi, Placa, Renavam, Leilão
10/06/2025 20:08:08
Ativo

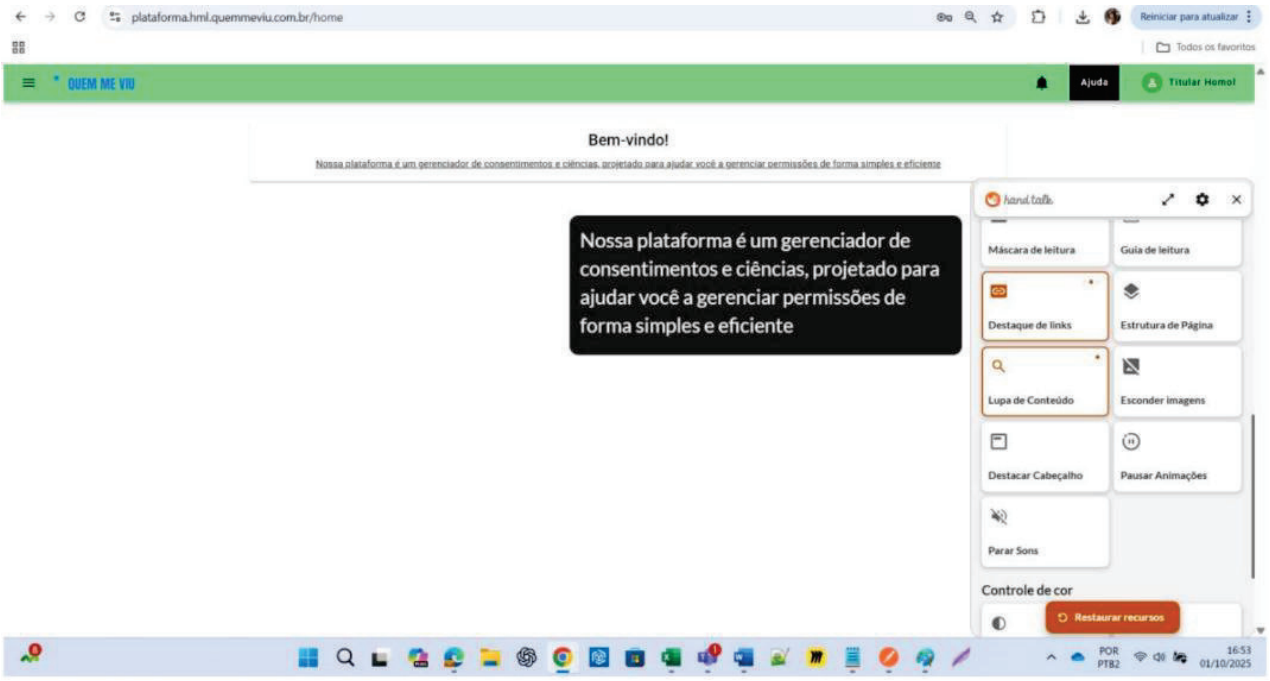

QUEM ME VIU
Ajuda
Titular teste postman
Compartilhamentos
Meus Pedidos
CNPJ
Razão Social
Status
Período
Data de vencimento
BUSCAR
EXPORTAR
Razão Social / CNPJ
Base Legal
Dados
Data Solicitação
Data Vencimento
Status
Empresa Time Produtos Teckey 22.086.298/0001-37
Consentimento do titular dos dados
CPF do condutor, Data de nascimento, Descrição do sexo, Descrição localidade de nascimento, Endereço logradouro, Nome condutor, Nome do pai, Número de documento, Órgão expedidor do documento, UF expedidor do documento, Nacionalidade, Data de validade CNH, Situação CNH, Nome da mãe, Número Registro
11/06/2025 09:19:53
26/06/2025 09:19:53
Negado
CPF do condutor, Data de nascimento, Descrição do sexo, Endereço logradouro, Nome condutor, Nome do pai, Número de documento, Órgão expedidor do documento, UF expedidor do documento, Data de validade CNH, Situação CNH, Nome da mãe, Ano fabricação, Ano modelo, Chassi, Placa, Renavam, Leilão
11/06/2025 09:19:52
26/06/2025 09:19:52
Expirado
Mostrando de 1 a 2 de 2 registros.

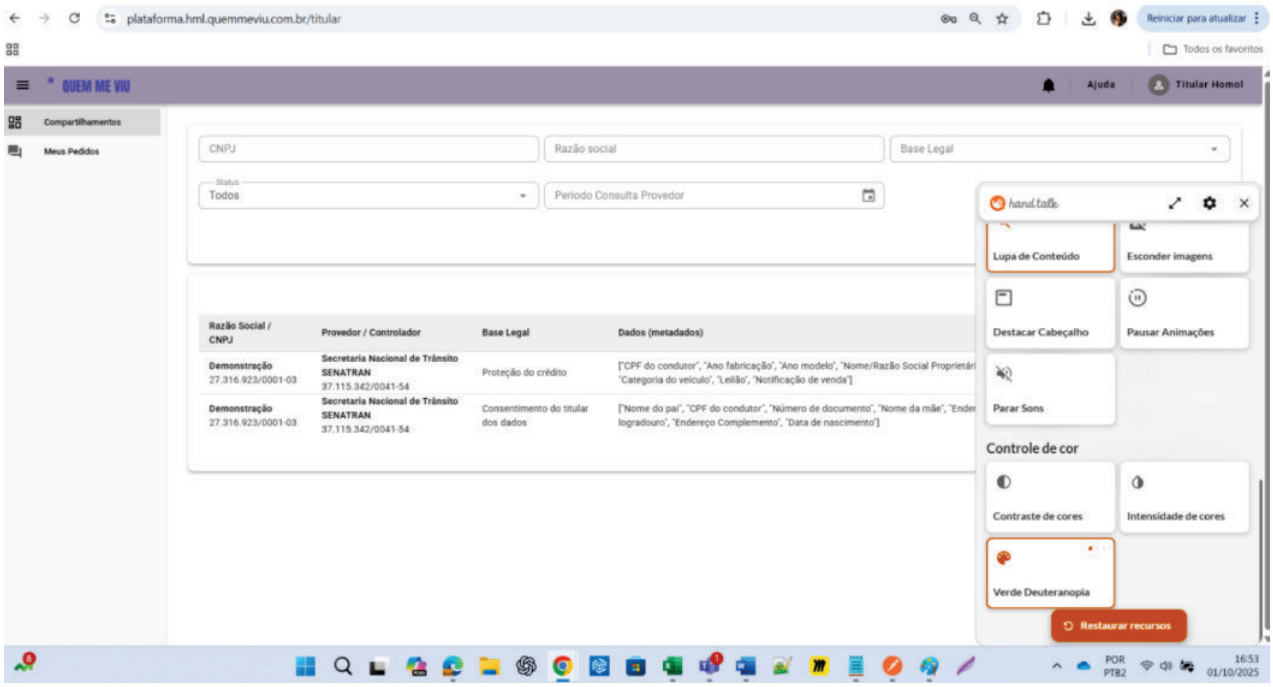

plataforma.hml.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Homol
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Assistente de IA
Sinônimos e significados
Controle de fonte
Tamanho de fonte
Estilo de texto
Letras Destacadas
Espaço entre linhas
Espaço entre letras
Navegação
Restaurar recursos


plataforma.hml.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Homol
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Assistente de IA
Sinônimos e significados
Controle de fonte
Tamanho de fonte
Estilo de texto
Letras Destacadas
Espaço entre linhas
Espaço entre letras
Navegação
Restaurar recursos


plataforma.hml.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Homol
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Letras Destacadas
Espaço entre linhas
Espaço entre letras
Navegação
Leitor de sites
Modo de leitura
Máscara de leitura
Guia de leitura
Destaque de links
Estrutura de Página
Restaurar recursos


plataforma.hml.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Homol
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Máscara de leitura
Guia de leitura
Destaque de links
Estrutura de Página
Lupa de Conteúdo
Esconder Imagens
Destacar Cabeçalho
Pausar Animações
Parar Sons
Controle de cor
Restaurar recursos


plataforma.hml.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Homol
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
hand talk
Máscara de leitura
Guia de leitura
Destaque de links
Estrutura de Página
Lupa de Conteúdo
Esconder imagens
Destacar Cabeçalho
Pausar Animações
Parar Sons
Controle de cor
Restaurar recursos


plataforma.hml.quemmeviu.com.br/titular
QUEM ME VIU
Ajuda
Titular Homol
Compartilhamentos
Meus Pedidos
CNPJ
Razão social
Base Legal
Status
Todos
Período Consulta Provedor
Razão Social / CNPJ
Provedor / Controlador
Base Legal
Dados (metadados)
Demonstração 27.316.923/0001-03
Secretaria Nacional de Trânsito SENATRAN 37.115.342/0041-54
Proteção do crédito
Demonstração 27.316.923/0001-03
Secretaria Nacional de Trânsito SENATRAN 37.115.342/0041-54
Consentimento do titular dos dados
hand talk
Lupa de Conteúdo
Esconder imagens
Destacar Cabeçalho
Pausar Animações
Parar Sons
Controle de cor
Contraste de cores
Intensidade de cores
Verde Deuteranopia
Restaurar recursos

4. Histórico de alterações

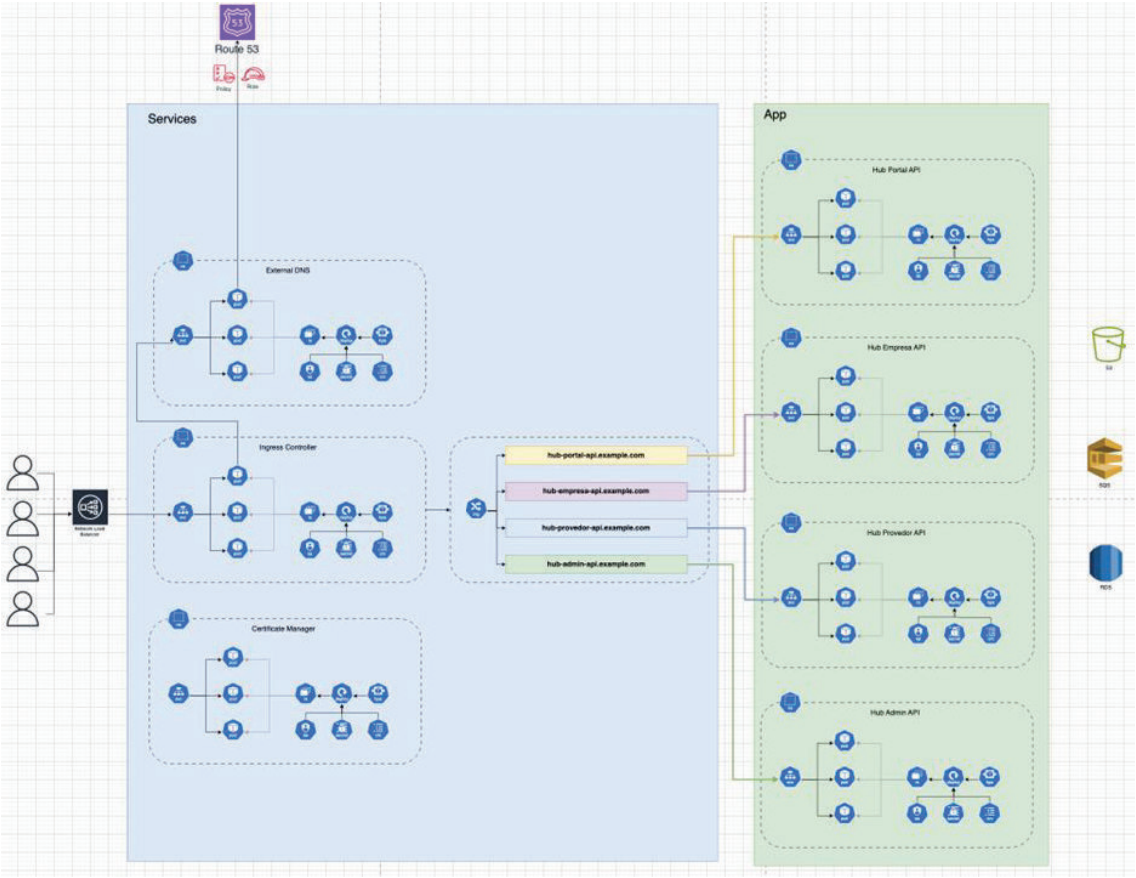
VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

1. Descrição

A solução oferece capacidade de auto scaling para ajustar recursos de forma dinâmica conforme a demanda, garantindo alta disponibilidade e performance. Conta com mecanismos robustos de disaster recovery para assegurar continuidade operacional em cenários críticos. Além disso, disponibiliza controle de acesso granular, permitindo definir permissões detalhadas por usuário ou grupo, aliado a logs e trilhas completas para auditoria e conformidade.

2. Auto scaling, disaster recovery

Para implementação da escalabilidade e resiliência fazemos uso do Kubernates, 100% integrado com mecanismos de segurança como firewall, waf, entre outros. A Firewall e o WAF usados são da AWS.



O Disaster Recovery, está implementado em modo HOT estando garantindo a distribuição do Kubernets e do Banco de dados em pelo menos duas Zonas distintas da AWS. Os componentes S3 e SQS já implementam nativamente Alta Disponibilidade e Disaster Recovery. Esta arquitetura, garante o Load Balance (LB - balanceamento), High-Availablity (HA – alta disponibilidade) e Disaster Recovery (DR – recuperação de desastres).

Adicionalmente a esta arquitetura, encontrase configurado toda a estrutura em Terraform, para levantamento do ambiente em modo COLD em qualquer outra região da AWS ou mesmo fora do Brasil para situação emergencial critica.

```
bash-3.2$ terraform init
Initializing the backend...
Initializing modules...
Initializing provider plugins...
- Reusing previous version of hashicorp/helm from the dependency lock file
- Reusing previous version of hashicorp/kubernetes from the dependency lock file
- Reusing previous version of hashicorp/aws from the dependency lock file
- Reusing previous version of hashicorp/tls from the dependency lock file
- Reusing previous version of hashicorp/random from the dependency lock file
- Reusing previous version of hashicorp/null from the dependency lock file
- Reusing previous version of hashicorp/cloudinit from the dependency lock file
- Using previously-installed hashicorp/tls v4.1.0
- Using previously-installed hashicorp/random v3.7.2
- Using previously-installed hashicorp/null v3.2.4
- Using previously-installed hashicorp/cloudinit v2.3.7
- Using previously-installed hashicorp/helm v3.0.2
- Using previously-installed hashicorp/kubernetes v2.38.0
- Using previously-installed hashicorp/aws v5.100.0

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
bash-3.2$ terraform output
eks_cluster_name = "gcc-tst-eks"
eks_nodes_sg_id = [
  "sg-0a4b9aa105ad4c16d",
]
eks_oidc_issuer_url = "https://oidc.eks.us-east-1.amazonaws.com/id/574A4B097775F457FFC822C5EA868665"
eks_oidc_thumbprint = "9e99a48a9960b14926bb7f3b02e22da2b0ab7280"
elasticache_auth_token = <sensitive>
elasticache_cluster_address = [
  "master.gcc-tst-redis-replication-group.za3zsr.use1.cache.amazonaws.com",
]
elasticache_cluster_arn = [
  "arn:aws:elasticache:us-east-1:018535004794:replicationgroup:gcc-tst-redis-replication-group",
]
elasticache_cluster_port = [
  6379,
]
irsa_sqs_role_arn = "arn:aws:iam::018535004794:role/gcc-tst-irsa-sqs"
rds_db_name = ""
rds_endpoint = "gcc-tst-rds-postgres.cc34y8wkctt2.us-east-1.rds.amazonaws.com:5432"
rds_password = <sensitive>
rds_port = 5432
rds_username = "adminuser"
s3_bucket_arn = {
  "gcc-tst-hub-files" = "arn:aws:s3:::gcc-tst-hub-files"
  "gcc-tst-logs-sqs" = "arn:aws:s3:::gcc-tst-logs-sqs"
}
s3_bucket_endpoint = {
  "gcc-tst-hub-files" = "gcc-tst-hub-files.s3.amazonaws.com"
  "gcc-tst-logs-sqs" = "gcc-tst-logs-sqs.s3.amazonaws.com"
}
sqs_queue_arn = [
  "arn:aws:sqs:us-east-1:018535004794:gcc-tst-dlq",
  "arn:aws:sqs:us-east-1:018535004794:gcc-tst-gerador-hash",
  "arn:aws:sqs:us-east-1:018535004794:gcc-tst-hash-consumer",
  "arn:aws:sqs:us-east-1:018535004794:gcc-tst-notifications",
  "arn:aws:sqs:us-east-1:018535004794:update-cache",
]
sqs_queue_name = [
  "gcc-tst-dlq",
  "gcc-tst-gerador-hash",
  "gcc-tst-hash-consumer",
  "gcc-tst-notifications",
  "update-cache",
]
sqs_queue_url = [
  "https://sqs.us-east-1.amazonaws.com/018535004794/gcc-tst-dlq",
  "https://sqs.us-east-1.amazonaws.com/018535004794/gcc-tst-gerador-hash",
  "https://sqs.us-east-1.amazonaws.com/018535004794/gcc-tst-hash-consumer",
  "https://sqs.us-east-1.amazonaws.com/018535004794/gcc-tst-notifications",
  "https://sqs.us-east-1.amazonaws.com/018535004794/update-cache",
]
bash-3.2$
```

3. Arquitetura

1. Disponibilidade e Continuidade Operacional

A arquitetura da plataforma foi concebida para garantir alta disponibilidade (HA) e continuidade de serviço em conformidade com as melhores práticas da AWS Well-Architected Framework.

Os principais mecanismos implementados são os seguintes:

1.1. Disaster Recovery (Recuperação de Desastres)

• O ambiente encontra-se implementado em modo HOT DR, com distribuição automática dos clusters Kubernetes e das instâncias de banco de dados em múltiplas Availability Zones (AZs) da AWS, garantindo redundância geográfica e tolerância a falhas.

• Os serviços Amazon S3 e Amazon SQS contam com replicação e recuperação de desastres nativa, assegurando a persistência e integridade dos dados em caso de incidentes críticos.
• Adicionalmente, a infraestrutura é definida em Terraform (Infraestrutura como Código), permitindo o provisionamento rápido em modo COLD DR em qualquer outra região AWS — ou até mesmo fora do território nacional — em situações de contingência severa.
1.2. Balanceamento de Carga (Load Balancing)
• Todos os componentes da plataforma implementam mecanismos de balanceamento de carga para otimização de desempenho e continuidade de serviço.
• Os portais, APIs e microserviços são balanceados via Kubernetes (Ingress Controller), que utiliza o AWS Network Load Balancer (NLB) para distribuir o tráfego de forma eficiente e segura.
• Os serviços RDS, SQS e S3 utilizam balanceamento nativo da AWS, garantindo distribuição inteligente de requisições e resiliência a picos de carga.
1.3. Alta Disponibilidade (High Availability)
• Todos os componentes críticos são configurados em modo redundante.
• A camada de aplicação, os serviços e APIs estão em pods replicados no Kubernetes, enquanto o banco de dados e demais serviços AWS (SQS, S3) contam com mecanismos automáticos de failover.
• Monitorização contínua e métricas de saúde garantem que qualquer instância degradada seja automaticamente substituída.

2. Escalabilidade e Performance
A plataforma foi desenhada para crescer horizontal e verticalmente, adaptando-se automaticamente à variação da carga de trabalho.
2.1. Auto Scaling
• O Kubernetes Horizontal Pod Autoscaler (HPA) está configurado para escalar automaticamente os pods quando a utilização atinge 75% de carga, permitindo o crescimento antes da saturação do sistema.
• O Cluster Autoscaler garante a criação de novos nós (nodes) de forma dinâmica, assegurando disponibilidade mesmo durante picos de tráfego.
2.2. Escalabilidade de Serviços AWS
• Amazon SQS e Amazon S3 implementam escalabilidade horizontal nativa, suportando alto débito e elevada concorrência sem necessidade de intervenção manual.
• O Amazon RDS encontra-se configurado com auto scaling de armazenamento e monitorização de métricas de CPU e memória, permitindo o aumento automático da capacidade conforme o crescimento da demanda.

2.3. Monitorização e Observabilidade
• O ambiente é monitorizado em tempo real através do Amazon CloudWatch, com alarmes proativos configurados para métricas de desempenho, capacidade e disponibilidade.
• Logs e métricas são agregados e analisados periodicamente para ajustes de performance e otimização de custos.

3. Segurança e Conformidade

A plataforma adota uma abordagem "Security by Design", garantindo a proteção de dados, comunicações e infraestrutura desde o desenvolvimento até a operação.

3.1. Proteção de Dados

• Dados em trânsito: protegidos com TLS 1.3 (TLS_AES_256_GCM_SHA384) em todas as comunicações externas e internas.

• Dados em repouso: criptografados via AWS KMS (Key Management Service), abrangendo S3, SQS e RDS, com gestão centralizada de chaves e rotação automática.

3.2. Proteção de Aplicações e APIs

• Implementação do AWS Web Application Firewall (WAF) para defesa contra ameaças em camada de aplicação, incluindo:

o SQL Injection

o Cross-Site Scripting (XSS)

o Remote File Inclusion

o Brute Force e ataques automatizados

• Integração com AWS Shield para proteção avançada contra:

o DDoS volumétricos

o Protocol Attacks (SYN Flood, ACK Flood, Fragmentation)

o Reflection/Amplification Attacks

3.3. Segurança de Rede

• Segmentação lógica das redes por ambiente (produção, homologação, desenvolvimento), garantindo isolamento total entre camadas.

• Security Groups e Network ACLs configurados com princípio de privilégio mínimo, restringindo comunicações a portas e IPs específicos.

• Integração com VPC Endpoints para comunicações seguras com serviços internos da AWS sem exposição pública.

3.4. Segurança no Ciclo de Desenvolvimento

• Processo de CI/CD seguro, com:

o Repositórios Git isolados e segregados por ambiente.

o Pipelines automatizados com validações de código, testes e escaneamento de vulnerabilidades.

o Deploy controlado com validação de integridade e rollback automático em caso de falha.

4. Conclusão

A arquitetura descrita combina resiliência operacional, elasticidade e segurança avançada, assegurando:

• Alta disponibilidade e recuperação automática de falhas;

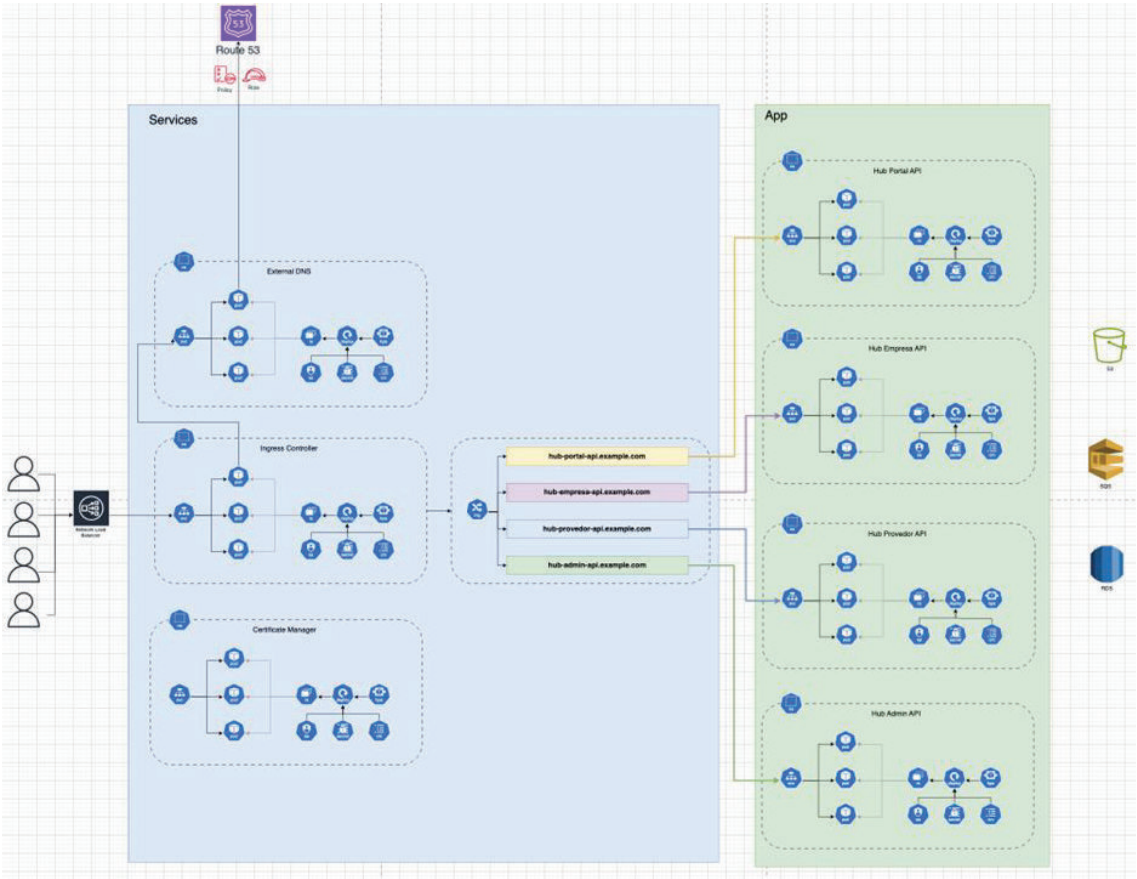
• Escalabilidade contínua e sob demanda;

• Proteção integral contra ameaças de rede e aplicação;

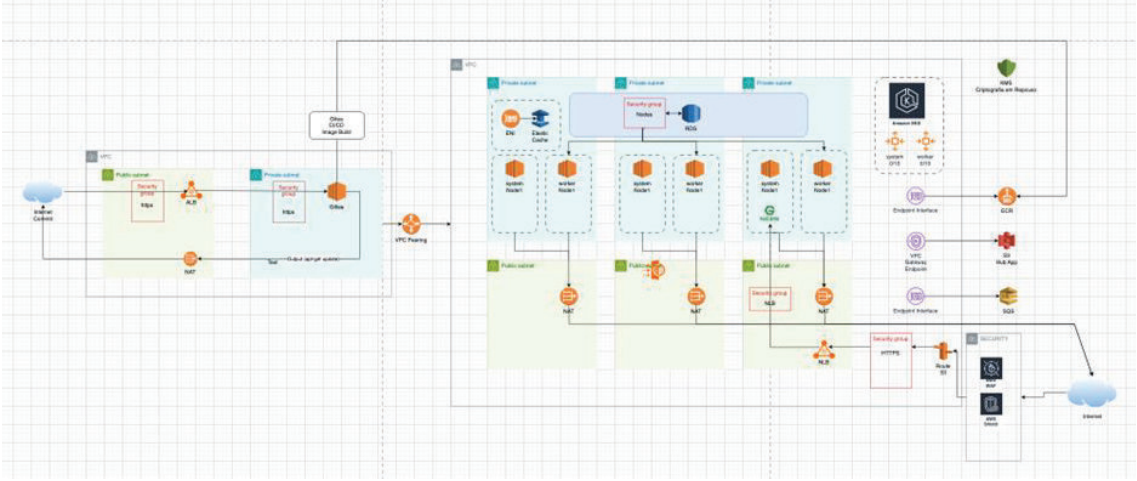
• Conformidade com os princípios da AWS Well-Architected Framework (Pilares de Reliability, Performance Efficiency e Security).

Esta combinação garante que a plataforma se mantém disponível, segura e eficiente mesmo sob cenários de alta carga, falhas regionais ou ameaças externas.

Para implementação da escalabilidade e resiliência fazemos uso do Kubernates, 100% integrado com mecanismos de segurança como firewall, waf, entre outros. A Firewall e o WAF usados são da AWS.



Abaixo detalhamos, a arquitetura que permite a escalabilidade, segurança e resiliência de cada um dos Hubs implementados.

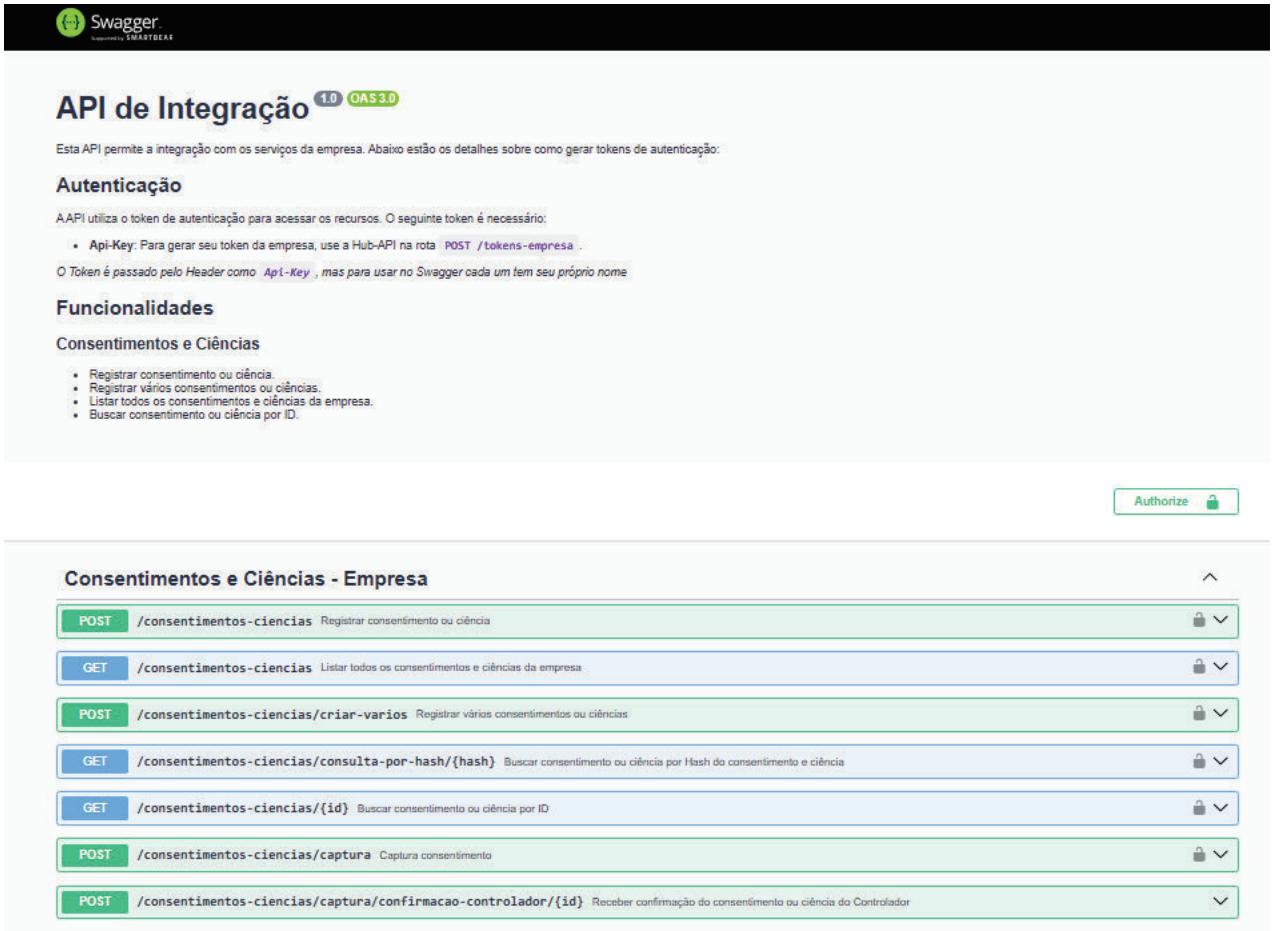


4. Swagger/OpenAPI

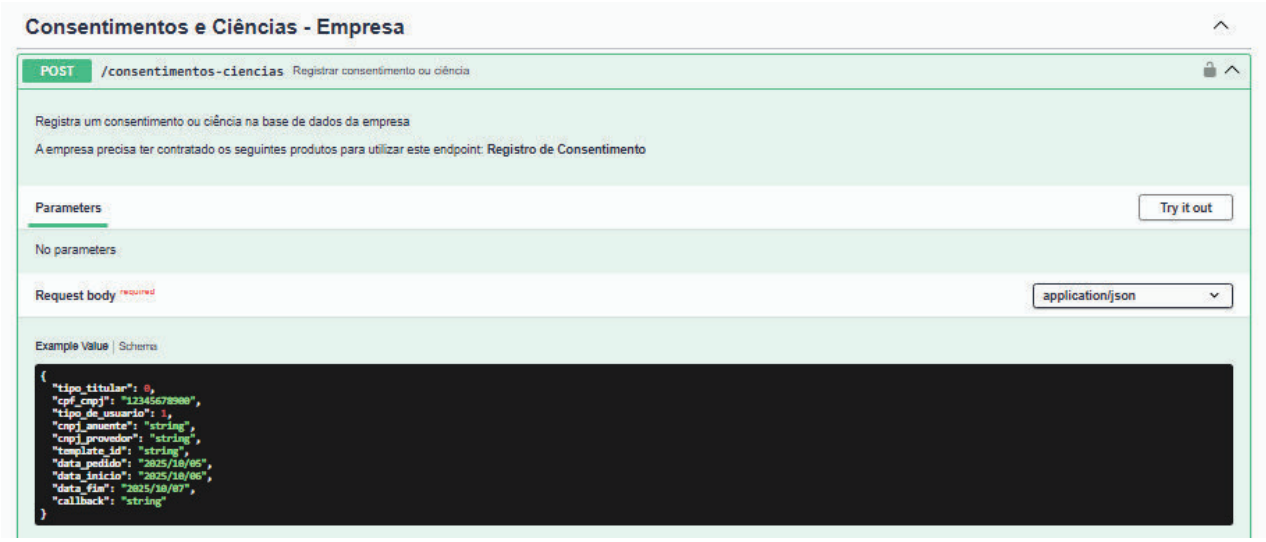
O Swagger da API Company possui um conjunto de ferramentas que facilita a documentação,
teste e integração de APIs REST. Ele utiliza a especificação OpenAPI, um padrão aberto para
descrever APIs de forma estruturada e legível tanto por humanos quanto por máquinas.

Abaixo prints dos endpoints da nossa API:

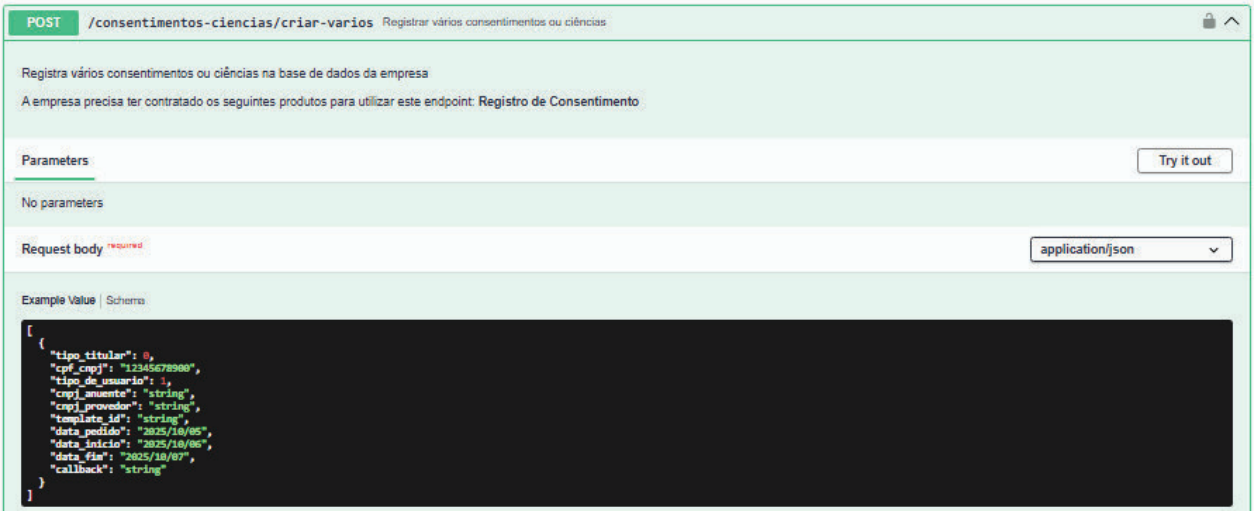
Link https://company.hml.quemmeviu.com.br/api



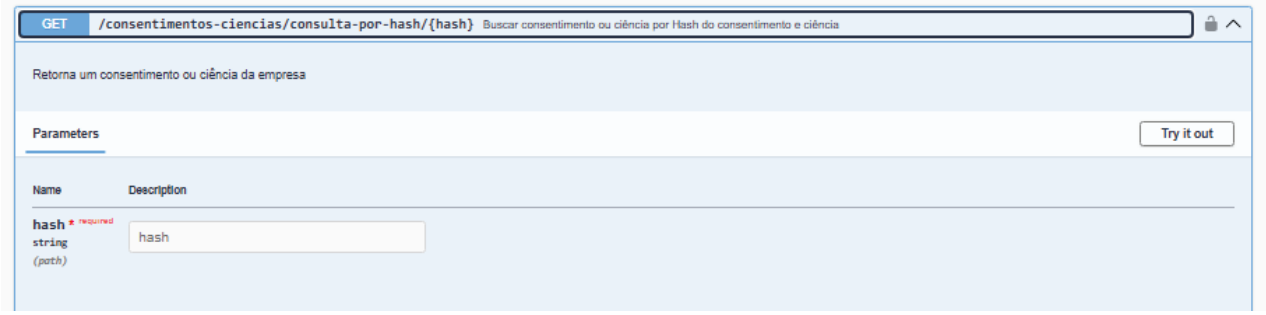
API Registro de consentimento e ciência



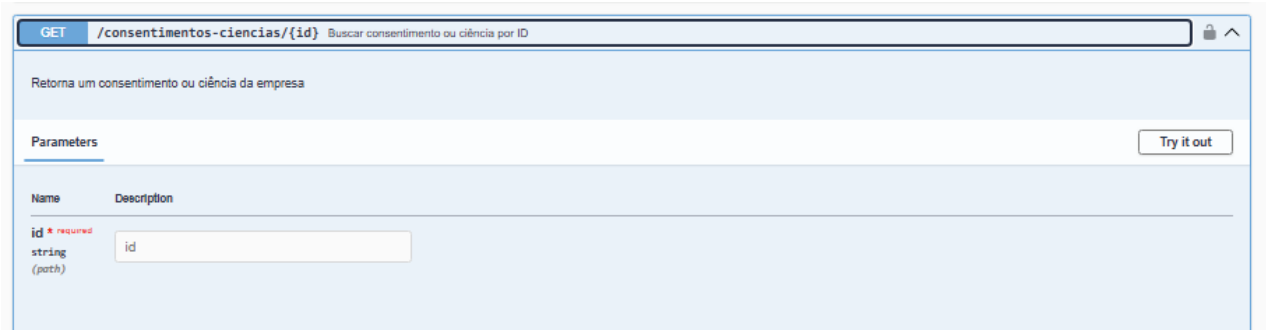
API registro de consentimento e ciência (vários)



API consulta pro meio do Hash



API consulta por meio do ID



API captura de consentimento

5. HISTÓRICO DE ALTERAÇÃO

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

1. Objetivo

A GCC possui mecanismos para gerar e gerenciar hash criptográficos únicos, assegurando:
• Integridade dos dados, evitando alterações não autorizadas.
• Autenticidade e rastreabilidade, permitindo validação segura de informações e transações.
• Proteção contra fraudes, por meio de algoritmos robustos e irreversíveis (ex.: SHA256).
• Gestão eficiente, com controle sobre criação, armazenamento e verificação dos hashes.
• Conformidade com padrões de segurança, garantindo aderência às melhores práticas e normas regulatórias.

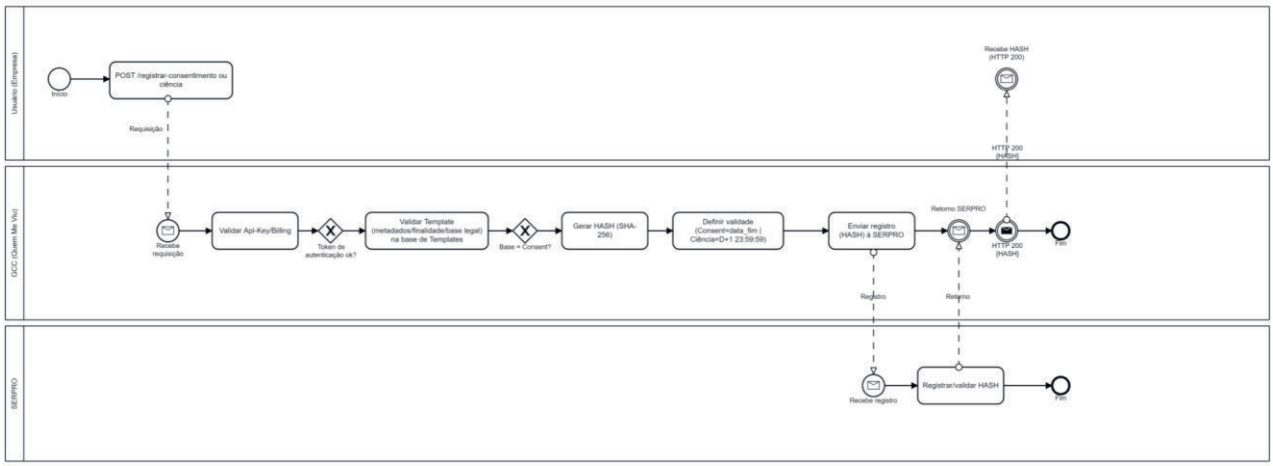
2. Controle do Hash

O hash gerado pela GCC é compatível com os padrões exigidos e utiliza o algoritmo SHA-256, reconhecido internacionalmente por sua robustez e confiabilidade. Benefícios:
• Alta segurança: SHA-256 é um algoritmo irreversível, dificultando ataques de força bruta e garantindo integridade dos dados.
• Conformidade com normas: Atende aos padrões exigidos por regulamentações e boas práticas de segurança.
• Proteção contra fraudes: Garante que dados não sejam alterados sem detecção.
• Escalabilidade e interoperabilidade: Pode ser aplicado em diferentes sistemas e processos sem comprometer desempenho.
• Rastreabilidade confiável: Permite validação segura de transações e informações.

Exemplo do modelo de concatenação dos dados:
• Data e hora do pedido do Hash (request)
• Data e hora do response do Hash (geração)
• Tipo de Pessoa: PF ou PJ
• CPF/ CNPJ Titular
• ID Template
• Consentimento: True ou False
• CNPJ do requerente (usuário)
• CNPJ Anuente
• CNPJ GCC
• Código de transação
• Data do pedido do consentimento
• Data da autorização do consentimento (Data início)
• Data Expiração Hash (data fim consentimento)/quando for ciência 24 horas

3. BPMN Fluxo de registro de consentimento e ciência

O BPMN (Business Process Model and Notation) abaixo demonstra a forma padronizada e visual do fluxo de registro de consentimento e ciência onde ocorre a geração do HASH.

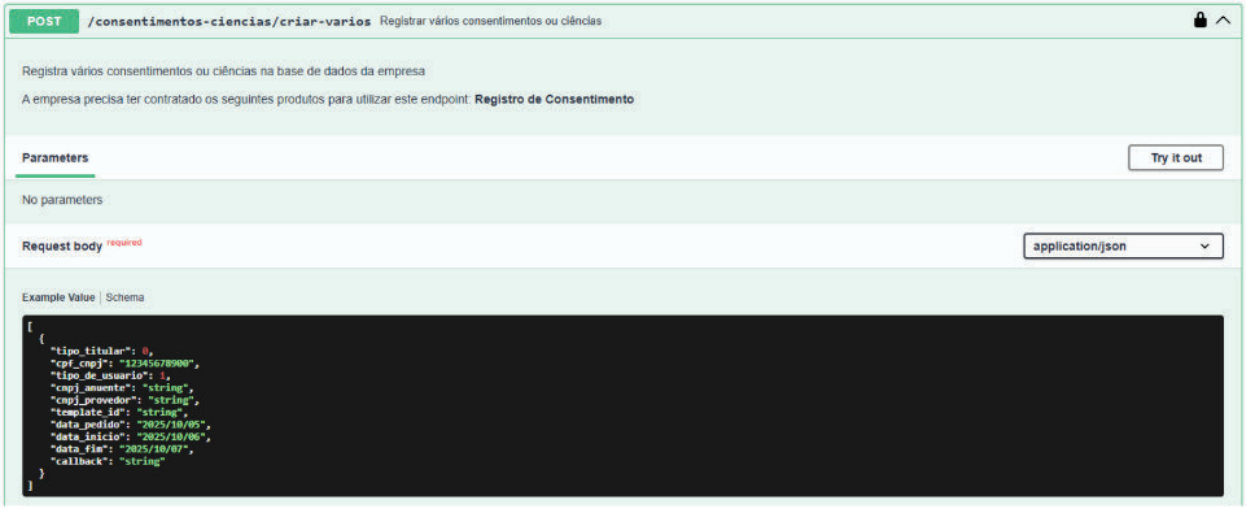


4. Capacidade gerar arquivos batch

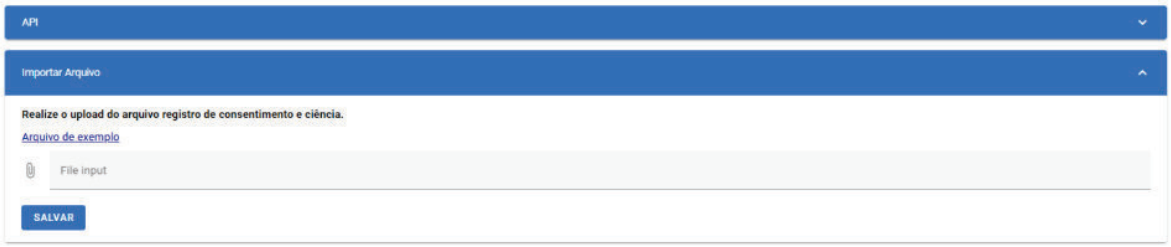
A principal vantagem da solução da GCC ao permitir a geração de arquivos batch é a automação e padronização de processos repetitivos, trazendo ganhos significativos em eficiência operacional.

Exemplo via API

O endpoint /consentimentos-ciencias/criar-varios possibilita incluir vários registros, independente da base legal ou tipo de pessoa (PF/PJ), de uma única vez por meio de lista.



Exemplo plataforma de usuário empresa (clientes)
Possibilitamos aos usuários os registros de consentimentos e ciências via arquivo através da plataforma de empresa, área integrações.
URL https://plataforma.hml.quemmeviu.com.br/empresa/login

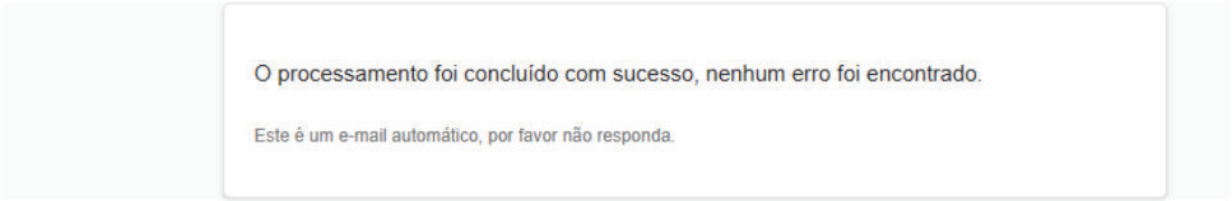


Arquivo exemplo

	A	B	C	D	E	F	G	H	I
1	tipo_titular	cpf_cnpj	tipo_usuario	cnpj_anuente	cnpj_provedor	template_id	data_pedido	data_inicio	data_fim
2	1	000.000.000-01	1		00.000.000/0000-03	100	21/10/2025	22/10/2025	23/10/2025
3	2	00.000.000/0000-01	2	00.000.000/0000-02	00.000.000/0000-03	200	18/10/2025	21/10/2025	21/10/2025
4									
5									
6									

Acompanhamento do processamento via e-mail

Para: polyana.silva+1@jb3ti.com.br



5. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

1. Descrição

Garantir que a gerenciadora de consentimentos e ciências disponha de estruturas e processos para atender às demandas de clientes e parceiros em diferentes áreas — negocial, comercial, técnica e jurídica — de forma ágil, segura e eficiente.

2. Objetivo

Demonstrar a estrutura organizacional e os canais de comunicação mantidos pela JB3 Softwares S/A para atendimento aos diferentes públicos — clientes corporativos, titulares de dados, parceiros, órgãos reguladores e público em geral — assegurando disponibilidade, rastreabilidade, tempo de resposta e níveis de atendimento conforme as boas práticas de governança e os requisitos técnicos de operação.

3. Estrutura de atendimento

A JB3 Softwares S/A mantém estrutura própria e dedicada às frentes negocial, comercial, técnico-operacional e jurídico-institucional, com fluxos de atendimento definidos e centralizados em sua plataforma corporativa.

Área	Responsável	E-mail Institucional	Finalidade
Negocial / Produtos	Renato Pedroso da Cruz – Gerente de Produtos	renato.pedroso@jb3ti.com.br	Relacionamento com parceiros e integrações
Comercial	Marcelo Gagliardi Cesar – Head Comercial	marcelog.cesar@jb3ti.com.br / comercial@jb3ti.com.br	Propostas, credenciamentos e parcerias comerciais
Jurídico / Compliance / LGPD	Etelvina de Souza Rodrigues – Head Jurídico	vina.rodrigues@jb3ti.com.br / juridico@jb3ti.com.br	Questões contratuais, legais e de privacidade de dados
Técnico / Suporte Operacional	Polyana Cyntia Pereira da Silva – Apoio Técnico	polyana.silva@jb3ti.com.br / suporte@jb3ti.com.br	Atendimento técnico, dúvidas e incidentes

4. Canais de atendimento

4.1 Canal Eletrônico 24x7

A JB3 mantém um chat integrado à ferramenta corporativa, disponível 24 horas por dia, 7 dias por semana, destinado a usuários e titulares de dados para solicitar suporte técnico, consultar status de solicitações e encaminhar chamados automáticos para análise da equipe técnica. O chat conta com triagem

automatizada (bot) e integra-se ao sistema de gerenciamento de tickets, garantindo rastreabilidade completa.

4.2 Canais Institucionais

Além do chat, a JB3 disponibiliza:

- E-mail geral de atendimento: atendimento@jb3ti.com.br
- Portal de chamados: acesso via área logada da plataforma corporativa
- Canal de ouvidoria: https://www.contatoseguro.com.br/jb3softwaresltda

5. Horários, Níveis e Critérios de Atendimento

A estrutura de atendimento da JB3 Softwares é composta por três níveis de suporte e opera com classificação de severidade e urgência, garantindo resposta e tratamento adequados a cada tipo de ocorrência.

Nível	Descrição	Responsável	Horário de Atendimento
N1 – Atendimento Automatizado / Chatbot (24x7)	Atendimento inicial via chat integrado à ferramenta, com respostas automáticas, base de conhecimento e abertura de chamados. Classifica automaticamente o tipo e a severidade do incidente.	Sistema automatizado	24x7
N2 – Atendimento Técnico Especializado	Triagem e solução de incidentes técnicos, falhas operacionais, acessos e integrações. Atuação conforme severidade.	Equipe Técnica e Analistas de Suporte	Segunda a sexta, das 08h00 às 18h00, com plantão remoto para emergências críticas
N3 – Atendimento Avançado / Desenvolvimento e Infraestrutura	Correções estruturais e falhas de alto impacto sistêmico. Atuação sob acionamento imediato em incidentes críticos.	Gestor de Tecnologia e Product Owner	Segunda a sexta, das 08h00 às 18h00, com escalonamento 24x7 em regime de sobreaviso

6. Classificação de severidade

Todos os incidentes são classificados automaticamente e confirmados pela equipe técnica segundo os critérios a seguir:

Nível de Severidade	Descrição	Tempo de Resposta Inicial	Tempo de Solução / Mitigação
Crítica (S1)	Indisponibilidade total do sistema, falha em login ou interrupção generalizada.	Até 30 minutos	Correção imediata (24x7) até mitigação completa
Alta (S2)	Falhas que impactam parcialmente o funcionamento de módulos específicos.	Até 1 hora útil	Até 8 horas úteis
Média (S3)	Problemas pontuais sem impacto sistêmico.	Até 4 horas úteis	Até 24 horas úteis
Baixa (S4)	Dúvidas, solicitações de melhoria ou suporte administrativo.	Até 1 dia útil	Conforme prioridade de backlog

7. Ações e Escalonamento

Incidentes críticos (S1) acionam plantão técnico remoto imediato, mesmo fora do horário comercial.
Todos os chamados são registrados no Sistema de Tickets da JB3, com número de protocolo, status e histórico completo.
O Gerente de Produtos e o Gestor de Tecnologia são automaticamente notificados em incidentes críticos.
Após correção, é emitido Relatório de Ocorrência e Mitigação (ROM) com causas e medidas preventivas.

8. Compromisso

A JB3 Softwares garante disponibilidade 24x7 para tratamento de falhas críticas e sistêmicas, assegurando que clientes e titulares não permaneçam sem suporte em situações de indisponibilidade. Todos os atendimentos seguem as políticas corporativas de segurança e privacidade.

9. Registro e Rastreamento

Todos os atendimentos — via chat, e-mail, portal ou ouvidoria — são registrados no Sistema de Gerenciamento de Tickets da JB3 (Service Desk), com número único de

protocolo, data/hora de abertura e encerramento, histórico de interações, responsável técnico e SLA.

10. Aprovações

Renato Pedroso – Gerente de Produtos
Marcelo Gagliardi Cesar – Head Comercial
Etelvina de Souza Rodrigues – Head Jurídico
Mario Stella – Analista de Segurança da Informação

11. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

1. Contexto e Fundamentação

Esta evidência técnica tem por objetivo comprovar a implementação dos mecanismos de **autenticação segura** e da **interoperabilidade** previstos no **Estudo Técnico Preliminar (ETP) nº 390004/33/2025**, especificamente em seus **itens 9.3 e 9.4**, que determinam:
ETP 9.3 – "O Gerenciamento de Consentimento e Ciência é um serviço integrado (...) mediante mecanismos de autenticação segura, interoperabilidade com sistemas públicos (como GOV.BR), integração com entes autorizados e geração de evidências eletrônicas imutáveis e rastreáveis (...)."
ETP 9.4.3 – "Implementação de mecanismos de autenticação e monitoramento que permitam verificar a legitimidade dos acessos e das operações realizadas."
ETP 9.4.1 – "Registro e disponibilização de informações de auditoria relativas às integrações realizadas por meio de APIs autorizadas."

2. Objetivo da Evidência

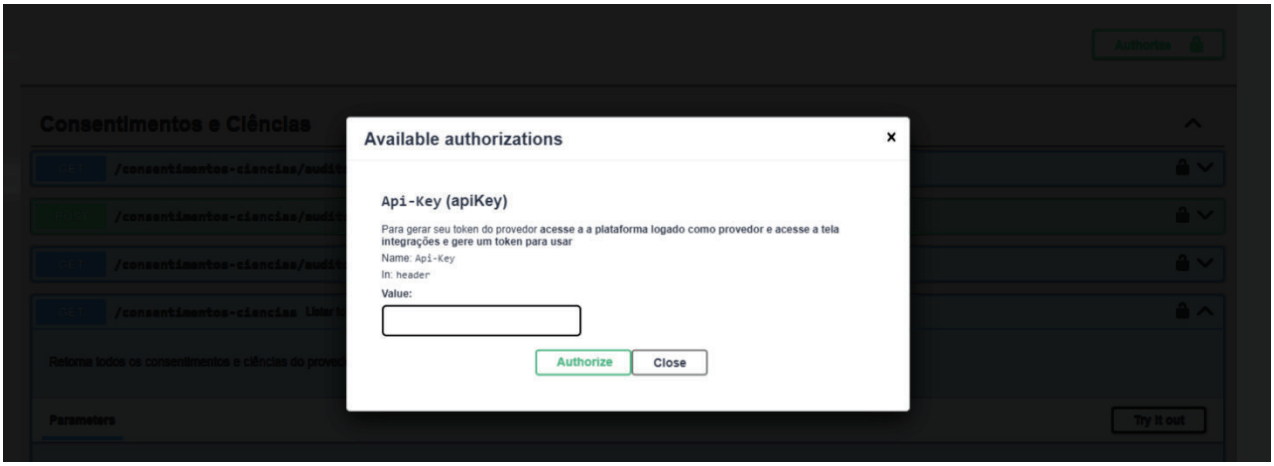
Demonstrar que a solução proposta implementa **autenticação segura**, **rastreabilidade de acessos**, **conformidade com padrões de API governamentais** e está **preparada para interoperar** com sistemas SENATRAN/SERPRO, GOV.BR e SEI, conforme previsto no ETP.

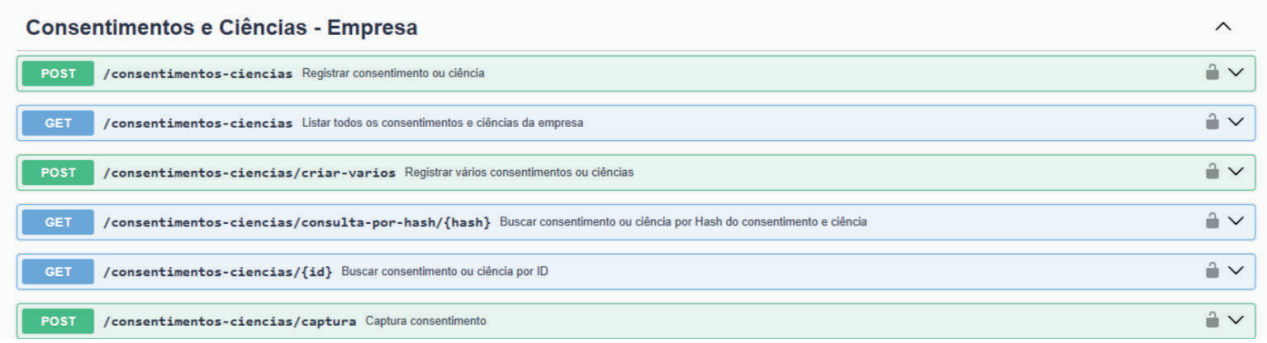
3. Mecanismo de Autenticação Segura (API Key + HTTPS)

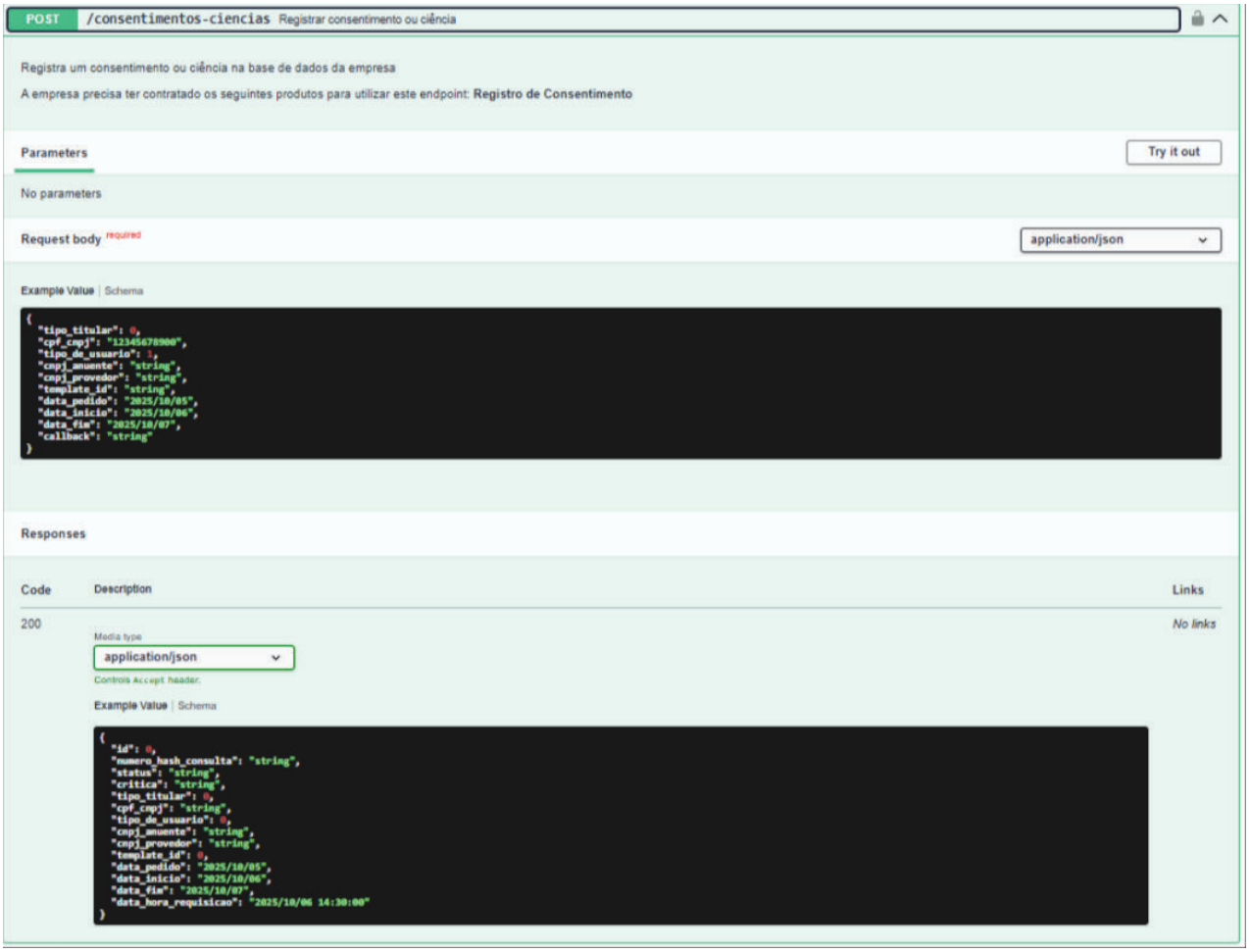
Sistema: Plataforma GCC (ambiente de homologacão)
Endereço: https://company.hml.quemmeviu.com.br/api
Protocolo: HTTPS (TLS 1.2 ou superior)
Tipo de autenticação: API Key individual por cliente/sistema
Algoritmo de geração: SHA-256 (aleatoriedade criptográfica)
Exemplo de requisição autenticada:
POST /api/endpoint
Host: company.hml.quemmeviu.com.br
Content-Type: application/json
Accept: application/json
Api-Key: 2d3eadcedadd5e3c9b8f66afac00412b1b91xxxxxxxxxxx

Cada chave é validada em tempo real, e o acesso é concedido somente após conferência em banco seguro criptografado.

Camadas de proteção:
- Tráfego 100% via HTTPS (TLS 1.2+);
- Armazenamento cifrado das chaves (AES-256);
- Escopo limitado de uso (por cliente e função);
- Política de rotação e revogação automática;
- Logs de auditoria por transação e IP de origem.


Consentimentos e Ciências
Available authorizations
Api-Key (apiKey)
Para gerar seu token do provedor acesse a a plataforma logado como provedor e acesse a tela integrações e gere um token para usar
Name: Api-Key
In: header
Value:
Authorize
Close
Parameters
Try it out


Consentimentos e Ciências - Empresa
POST /consentimentos-ciencias Registrar consentimento ou ciência
GET /consentimentos-ciencias Listar todos os consentimentos e ciências da empresa
POST /consentimentos-ciencias/criar-varios Registrar vários consentimentos ou ciências
GET /consentimentos-ciencias/consulta-por-hash/{hash} Buscar consentimento ou ciência por Hash do consentimento e ciência
GET /consentimentos-ciencias/{id} Buscar consentimento ou ciência por ID
POST /consentimentos-ciencias/captura Captura consentimento



4. Interoperabilidade SENATRAN / SERPRO / GOV.BR

A solução está estruturada para interoperar com sistemas públicos através de APIs seguras, aderentes às normas do **Padrão de API do Governo Digital (gov.br/api)**, com suporte aos protocolos **OAuth 2.0**, **OpenID Connect** e **JWT RS256**.

Arquitetura de integração planejada:

1. **GOV.BR** – autenticação de titulares e operadores via OpenID Connect, com obtenção de access_token e id_token.
2. **SENATRAN (Credencia)** – integração por meio de API REST para gestão de contratos e vínculos institucionais.
3. **SERPRO (PGCC)** – integração futura para transmissão e consulta de hashes, registro de consentimentos e ciências, conforme publicação de documentação técnica.

Esquema simplificado:

Usuário → GOV.BR (autenticação) → GCC → SENATRAN (Credencia) → SERPRO (PGCC)

A arquitetura segue o princípio da **autonomia de ambiente** (ETP 2.7.49–2.7.50), mantendo integração apenas via APIs seguras e padronizadas.

5. Logs e Auditoria (ETP 9.4.1)

Cada requisição autenticada gera um registro em banco imutável de logs contendo:

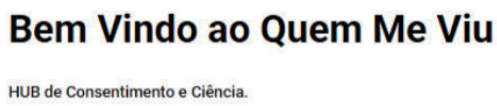
- Identificador da transação (UUID);
- Data/hora UTC;
- IP e user-agent de origem;
- Endpoint e método invocado;
- Hash SHA-256 do payload (para verificação de integridade);
- Resultado (sucesso/falha) e código HTTP.

Esses logs são versionados, assinados digitalmente e auditáveis por entidade externa, conforme princípios de rastreabilidade da LGPD e do ETP.

6. Conclusão

O ambiente avaliado implementa **mecanismos de autenticação segura**, com proteção criptográfica e controle de acesso granular, e está **preparado para interoperar** com os sistemas SENATRAN/SERPRO, GOV.BR.
Cumpre integralmente os princípios de **autenticidade, integridade, confidencialidade e rastreabilidade** exigidos pelo **ETP nº 390004/33/2025** e está aderente aos padrões do **Governo Digital Brasileiro** (gov.br/api).

7. Evidências



8. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

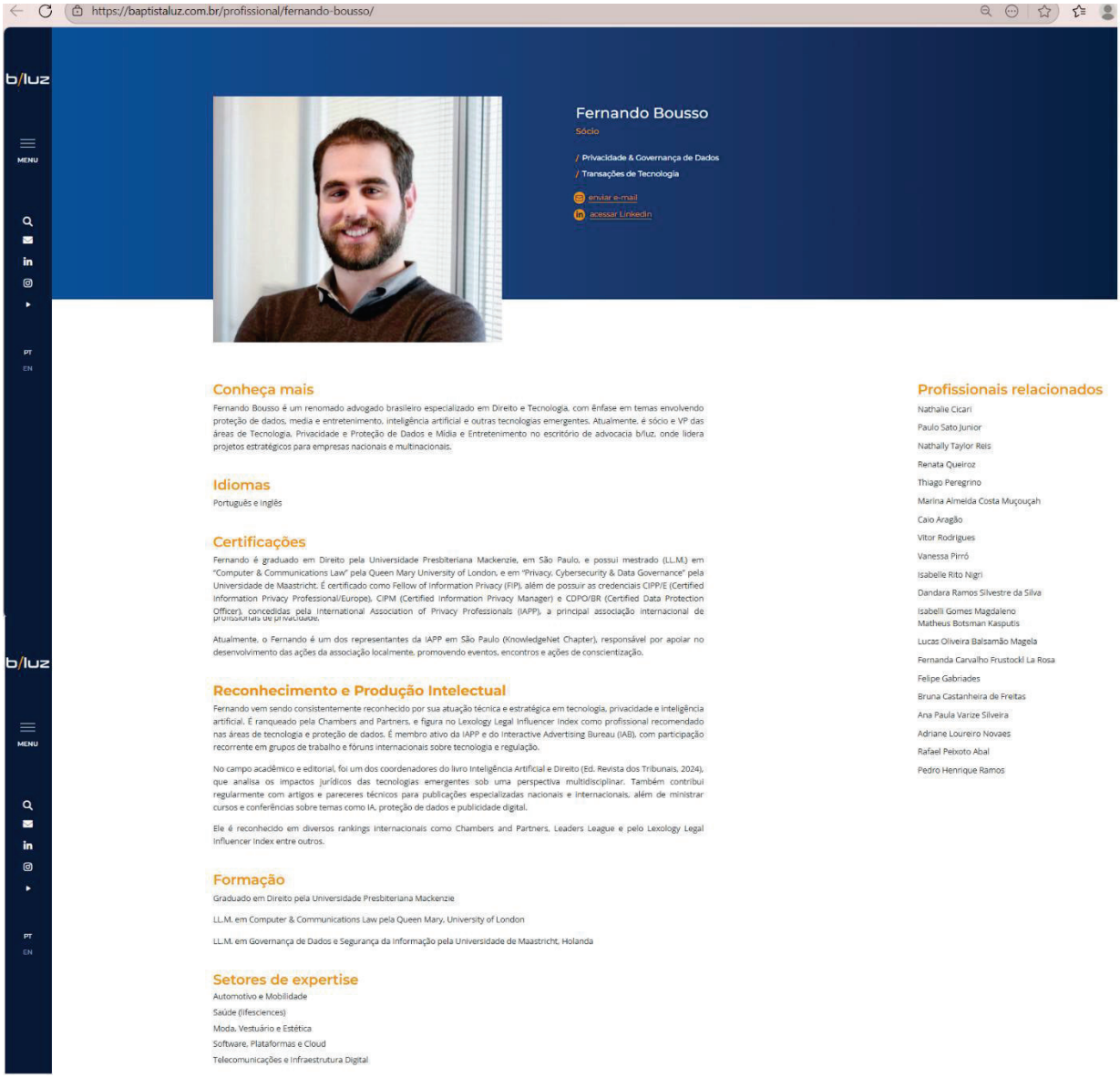
1. Descrição

Este documento assegura que a gerenciadora de consentimentos e ciências disponha de um Encarregado de Proteção de Dados (DPO) devidamente qualificado, conforme exigências da Lei Geral de Proteção de Dados (LGPD) e boas práticas de segurança da informação.

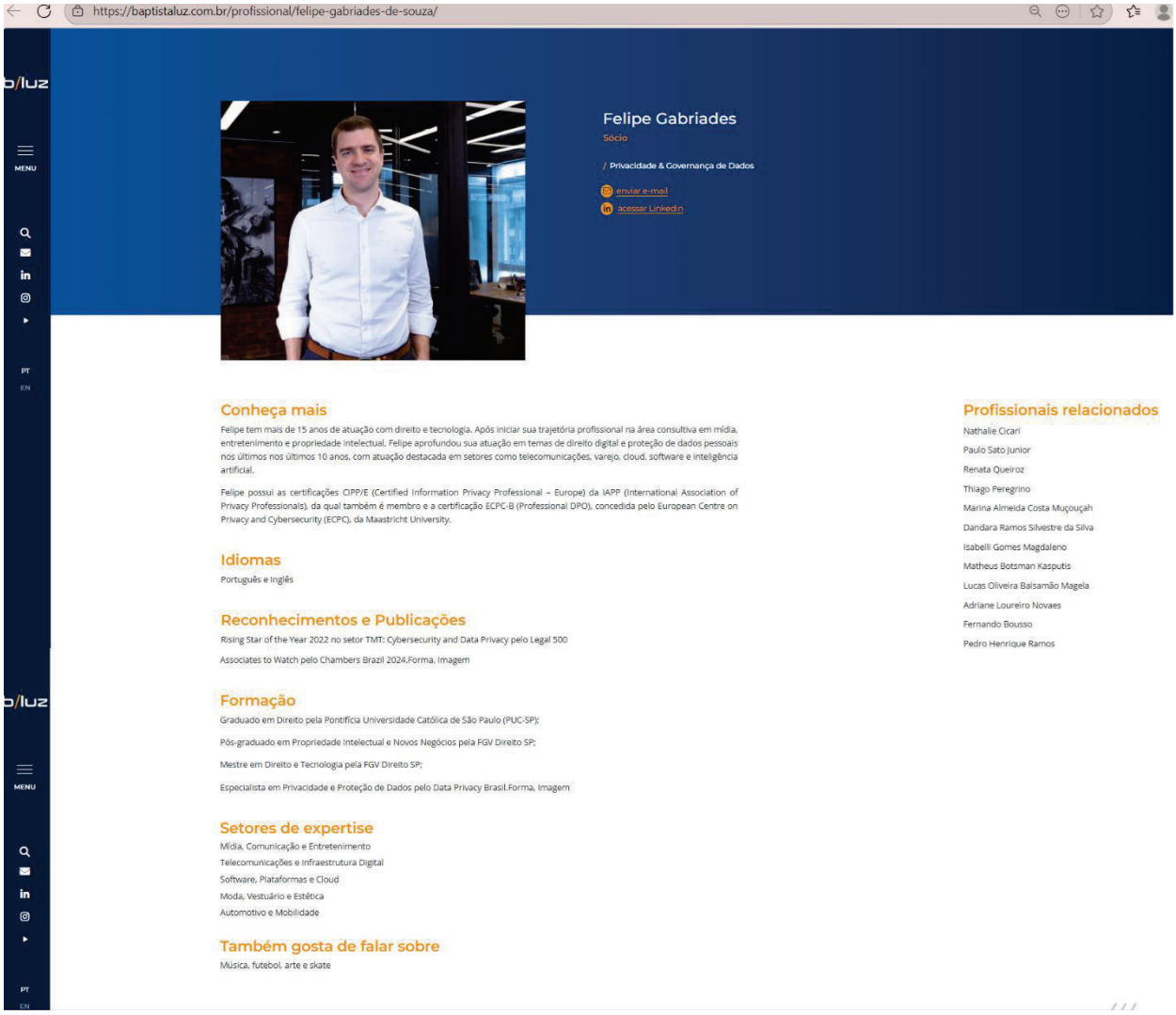
2. Qualificações DPO

Site público **https://baptistaluz.com.br/pessoas/**

https://baptistaluz.com.br/profissional/fernando-bousso



https://baptistaluz.com.br/profissional/felipe-gabriades-de-souza/



3. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

CÓDIGO DE CONDUTA, POLÍTICA DE COMPLIANCE E ANTISSUBORNO/ANTICORRUPÇÃO

1. Introdução

Este documento estabelece o Código de Conduta, a Política de Compliance e a Política Antissuborno e Anticorrupção da JB3 SOFTWARES S.A., integrando diretrizes éticas, legais e operacionais para garantir a conformidade com a legislação vigente, **em especial a Lei nº 12.846/2013 e seu regulamento atualizado pelo Decreto nº 11.129/2022**, prevenir riscos e promover a integridade nos negócios.

Seu objetivo é orientar todos os colaboradores, gestores, fornecedores, prestadores de serviços e parceiros sobre comportamentos e práticas aceitáveis e inaceitáveis no âmbito profissional, alinhados aos nossos valores.

2. Escopo e Abrangência

Esta política se aplica a:

Todos os empregados, diretores e administradores;

Prestadores de serviços, fornecedores e parceiros comerciais;

Qualquer terceiro que atue em nome ou interesse desta empresa.

O cumprimento desta política é obrigatório, independentemente do cargo, função ou local de trabalho.

3. Princípios e Valores Éticos

Além dos princípios já previstos, esta empresa adota, conforme previsto no Decreto nº 11.129/2022, os seguintes pilares de integridade:

- Comprometimento da Alta Direção com a cultura de integridade;
- Análise e gestão contínua de riscos de integridade;
- Códigos e políticas claras, de conhecimento público interno e externo;
- Treinamento contínuo e comunicação efetiva para todos os níveis hierárquicos;
- Canais de denúncia independentes, amplamente divulgados e protegidos contra retaliação;
- Monitoramento, auditoria e aperfeiçoamento contínuo do programa de integridade.

Ainda, e também importante:

Integridade: agir de forma honesta e justa;

Legalidade: respeitar todas as leis, normas e regulamentos aplicáveis;

Transparência: comunicar de forma clara, precisa e tempestiva;

Responsabilidade: assumir e responder pelos atos praticados;

Respeito às Pessoas: manter um ambiente de trabalho inclusivo, livre de assédio ou discriminação.

4. Compromisso da Alta Administração

A Alta Administração assegura o cumprimento dos requisitos do Decreto nº 11.129/2022, garantindo recursos e autonomia às áreas responsáveis pela implementação do Programa de Integridade, bem como apoiando e participando ativamente das ações preventivas, corretivas e de melhoria contínua.

Bem como, qualquer ato de represália contra denunciantes de boa-fé será punido com rigor.

5. Condutas Esperadas e Proibidas

5.1. Relacionamento com Clientes, Fornecedores e Parceiros

Cumprir contratos e prazos assumidos;

Não oferecer ou aceitar vantagens indevidas;

Manter negociações justas e transparentes.

5.2 Relação com Órgãos Públicos

É proibido oferecer, prometer ou autorizar pagamentos, benefícios ou vantagens a agentes públicos, direta ou indiretamente, com o objetivo de obter favorecimento;

Toda interação com autoridades deve ser registrada e documentada.

5.3 Conflito de Interesses

Evitar situações em que interesses pessoais possam prejudicar ou influenciar decisões corporativas;

Declarar qualquer potencial conflito ao Comitê de Compliance.

5.4 Suborno e Corrupção

Além do cumprimento integral da Lei nº 12.846/2013 e do Decreto nº 8.420/2015, esta empresa **observa as diretrizes atualizadas pelo Decreto nº 11.129/2022**, que reforça a necessidade de:

- Adoção de procedimentos internos que identifiquem e previnam práticas de corrupção;
- Implementação de controles internos específicos para monitorar transações com agentes públicos;
- Inclusão de cláusulas contratuais anticorrupção com fornecedores, prestadores e parceiros.

5.5 Lavagem de Dinheiro e Financiamento ao Terrorismo

É proibido participar, direta ou indiretamente, de operações que possam configurar lavagem de dinheiro ou financiamento ilícito.

5.6 Uso de Ativos e Recursos

Utilizar bens, equipamentos e recursos desta empresa apenas para fins corporativos legítimos;

Proibido o uso de informações internas para benefício próprio ou de terceiros.

6. Procedimentos de Compliance

Conforme o Decreto nº 11.129/2022, o Programa de Integridade desta empresa contempla:

- Avaliação periódica de riscos de integridade, levando em conta porte, estrutura e áreas de atuação;
- Due diligence de integridade prévia à contratação e renovação de contratos com terceiros;
- Treinamentos periódicos obrigatórios sobre ética, compliance, anticorrupção e prevenção à lavagem de dinheiro;
- Canal de denúncias independente, amplamente divulgado e acessível a todos;
- Mecanismos de proteção e confidencialidade para denunciantes;
- Auditorias internas e externas periódicas para verificar a efetividade das políticas.

7. Canal de Denúncias

Esta empresa mantém um canal seguro e confidencial para comunicação de violações:

Denúncias podem ser anônimas ou identificadas;

Garantia de não retaliação a denunciantes de boa-fé;

Investigação interna conduzida com imparcialidade e sigilo.

8. Gestão de Riscos e Monitoramento

A gestão de riscos seguirá os parâmetros estabelecidos pelo Decreto nº 11.129/2022, incluindo:

- Identificação e priorização de riscos de integridade;
- Definição de planos de ação para mitigação;
- Registro formal de medidas adotadas;
- Revisão anual das políticas e procedimentos com base nos resultados de monitoramento e auditorias.

9. Sanções Disciplinares

O descumprimento deste documento poderá resultar em:

Advertência formal;

Suspensão;

Desligamento por justa causa;

Encaminhamento às autoridades competentes, quando cabível.

10. Proteção de Dados e Privacidade

Cumprimento da Lei Geral de Proteção de Dados (Lei nº 13.709/2018);

Tratamento de dados pessoais apenas para finalidades legítimas e autorizadas.

11. Vigência e Revisão

Esta política entra em vigor na data de sua aprovação pela Diretoria desta empresa e será revisada anualmente ou sempre que houver mudanças legais ou estruturais relevantes.

12. Disposições Finais

Todos os colaboradores, prestadores de serviços, fornecedores e parceiros desta empresa devem formalizar seu conhecimento e concordância com este Código de Conduta, bem como com as políticas corporativas a eles vinculadas, por meio de assinatura do **Anexo I – Termo de Ciência e Compromisso**.

A Assinatura do termo é condição obrigatória para início ou continuidade da relação contratual, sendo certo que seu descumprimento poderá acarretar em medidas disciplinares e/ou legais cabíveis.

ANEXO I - Termo de Ciência e Compromisso

Eu, [Nome Completo], portador(a) do [Documento de Identidade], inscrito(a) no CPF sob nº [CPF], na qualidade de [Cargo/Função] junto à JB3 Softwares S.A., declaro que:

Tomei ciência integral do conteúdo do Código de Conduta, Política de Compliance e Política Antissuborno e Anticorrupção desta empresa, documento este que estabelece princípios éticos, regras de conduta e procedimentos internos para prevenção e combate à corrupção, fraudes, suborno, lavagem de dinheiro e demais irregularidades, **em conformidade com a Lei nº 12.846/2013, o Decreto nº 8.420/2015, o Decreto nº 11.129/2022 e demais legislações aplicáveis**.

Comprometo-me a cumprir todas as disposições nele previstas, observando estritamente as leis e regulamentos aplicáveis, inclusive a Lei nº 12.846/2013 (Lei Anticorrupção), o Decreto nº 8.420/2015, a Lei nº 13.709/2018 (LGPD) e demais normas pertinentes.

Abstenho-me de qualquer conduta que possa configurar violação ao presente documento, comprometendo-me a comunicar imediatamente, por meio dos canais oficiais da empresa, quaisquer irregularidades, suspeitas ou descumprimentos que cheguem ao meu conhecimento.

Reconheço que o descumprimento das disposições poderá resultar na aplicação das sanções disciplinares e legais cabíveis, inclusive rescisão contratual por justa causa e responsabilização civil e criminal.

Declaro que recebi um exemplar do documento e que tive oportunidade de esclarecer dúvidas com o setor competente antes da assinatura deste termo.

Local e data: _____

Assinatura: _____

Nome completo: _____

Cargo/Função: _____

13. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
CÓDIGO DE CONDUTA, POLÍTICA DE COMPLEANCE E POLÍTICA ANTISSUBORNO E ANTICORRUPÇÃO	Manual de Procedimentos	30/04/2025	1.0

Data	Descrição Ação	Versão	Responsável
30/04/2025	Elaboração	1.0	Jurídico
30/04/2025	Revisado e Aprovado	2.0	Diretoria Executiva

Classificação: Interno

DECLARAÇÃO FORMAL DE CONFORMIDADE E COMPROMISSO
(Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais)

JB3 SOFTWARES S.A., pessoa jurídica de direito privado, inscrita no CNPJ/MF sob o nº **58.493.015/0001-19**, com sede à Avenida Paulista, 2300 - Piso Pilotis - Sala 43 – Ed. São Luís Gonzaga - Consolação - São Paulo/SP - CEP:01310-300, neste ato representada por seu Sócio e Representante Legal, **JOSÉ ERNESTO MASCELLANI**, portador(a) do CPF nº 839.505.678-87 e RG nº 4.353.112 SSP/SP, DECLARA, para os devidos fins, que:

1. **Está ciente e cumpre integralmente** as disposições da Lei nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais – LGPD), bem como as regulamentações correlatas expedidas pela Autoridade Nacional de Proteção de Dados (ANPD) e demais órgãos competentes.
2. **Adota medidas técnicas e administrativas adequadas** para proteger dados pessoais contra acessos não autorizados, situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.
3. **Compromete-se** a utilizar dados pessoais estritamente para as finalidades legítimas, específicas e previamente informadas, observando os princípios da necessidade, adequação, transparência, livre acesso, qualidade dos dados, prevenção, não discriminação e responsabilização.
4. **Garante** que todos os colaboradores, prestadores de serviços, parceiros e subcontratados que tenham acesso a dados pessoais são devidamente treinados e orientados quanto ao cumprimento da LGPD, firmando, quando aplicável, instrumentos de confidencialidade e proteção de dados.
5. **Compromete-se** a atender, com eficiência e nos prazos legais, solicitações dos titulares de dados, bem como a cooperar com a ANPD e demais autoridades competentes em processos de fiscalização e auditoria.

6. **Reconhece** que o descumprimento da LGPD pode gerar responsabilidades administrativas, civis e penais, assumindo plena responsabilidade por eventuais danos decorrentes de sua inobservância.
7. **Atualização Contínua de Conformidade** – Compromete-se a revisar periodicamente suas políticas, procedimentos e controles internos relacionados ao tratamento de dados pessoais, realizando auditorias, testes de segurança e treinamentos contínuos, a fim de assegurar o alinhamento constante com a legislação vigente e com as boas práticas de governança em proteção de dados.

E por ser expressão da verdade, firma a presente Declaração para que produza seus efeitos legais.

São Paulo, 14 de outubro de 2025.

JOSÉ ERNESTO MASCELLANI

JOSÉ ERNESTO MASCELLANI
SÓCIO DIRETOR
JB3 SOFTWARES S.A.
CNPJ: 58.493.015/0001-19

Declaração Formal de Conformidade e Compromisso Lei LGPD.docx

Documento número #81e75c57-1828-49b8-98e8-a4172cbe9269

Hash do documento original (SHA256): 98e742d3401d3a33ba9e5c7758a1402b89a1e3615434e93c8e2acef717f6eef5

Assinaturas

JOSÉ ERNESTO MASCELLANI

CPF: 839.505.678-87

Assinou em 14 out 2025 às 16:57:24

JOSÉ ERNESTO MASCELLANI

Log

14 out 2025, 16:55:17	Operador com email vina.rodrigues@jb3ti.com.br na Conta 364adf64-8a29-49c8-b03b-b471ecdbc9dc criou este documento número 81e75c57-1828-49b8-98e8-a4172cbe9269. Data limite para assinatura do documento: 13 de novembro de 2025 (16:55). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
14 out 2025, 16:56:39	Operador com email vina.rodrigues@jb3ti.com.br na Conta 364adf64-8a29-49c8-b03b-b471ecdbc9dc alterou o processo de assinatura. Data limite para assinatura do documento: 16 de novembro de 2025 (17:19).
14 out 2025, 16:56:39	Operador com email vina.rodrigues@jb3ti.com.br na Conta 364adf64-8a29-49c8-b03b-b471ecdbc9dc adicionou à Lista de Assinatura: jose.ernesto@jb3ti.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; Assinatura manuscrita. Dados informados pelo Operador para validação do signatário: nome completo JOSÉ ERNESTO MASCELLANI e CPF 839.505.678-87.
14 out 2025, 16:57:24	JOSÉ ERNESTO MASCELLANI assinou. Pontos de autenticação: Token via E-mail jose.ernesto@jb3ti.com.br. CPF informado: 839.505.678-87. Assinatura manuscrita com hash SHA256 prefixo 8e0c29(...), vide anexo manuscript_14 out 2025, 16-57-12.png. IP: 179.110.203.246. Localização compartilhada pelo dispositivo eletrônico: latitude -22.9111316 e longitude -47.1691261. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão 1.1321.0 disponibilizado em https://app.clicksign.com.
14 out 2025, 16:57:27	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 81e75c57-1828-49b8-98e8-a4172cbe9269.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 81e75c57-1828-49b8-98e8-a4172cbe9269, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

Anexos

JOSÉ ERNESTO MASCELLANI

Assinou o documento em 14 out 2025 às 16:57:24

ASSINATURA MANUSCRITA
Assinatura manuscrita com hash SHA256 prefixo 8e0c29(...)

JOSÉ ERNESTO MASCELLANI
manuscript_14 out 2025, 16-57-12.png

1. Objetivo

Garantir que a gerenciadora de consentimentos e ciências comprove a existência de mecanismos robustos de controle de acesso e autenticação, assegurando:
• Proteção contra acessos não autorizados, por meio de autenticação segura
• Gestão de perfis e permissões, permitindo que usuários tenham acesso apenas às funcionalidades e dados compatíveis com seu papel.
• Rastreabilidade e auditoria, registrando todas as tentativas e ações para garantir transparência e conformidade.
• Conformidade com normas de segurança e LGPD, evitando riscos de vazamento ou uso indevido de informações.
• Integração com sistemas externos, mantendo interoperabilidade sem comprometer a segurança.

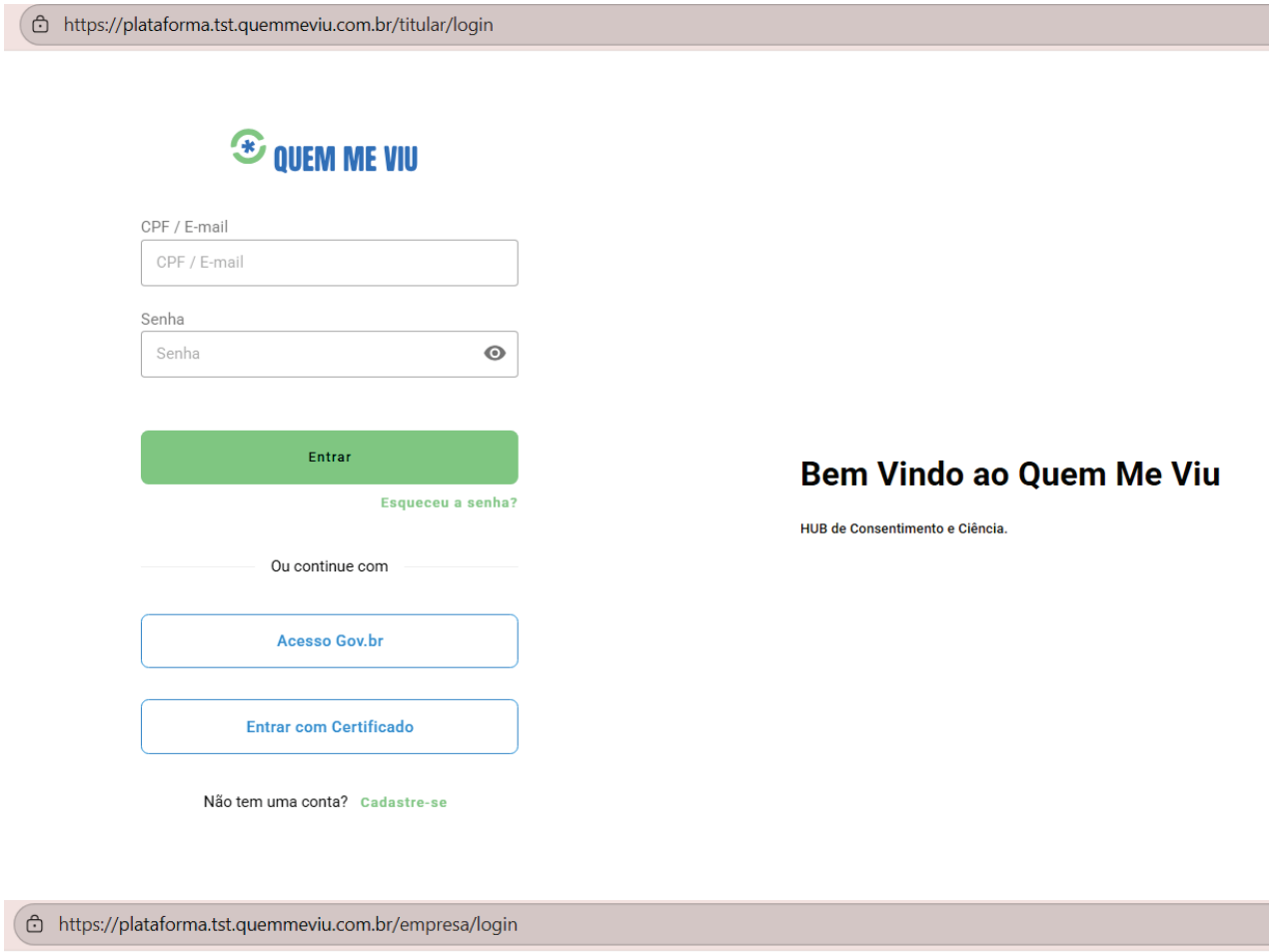
2. Controle de acesso

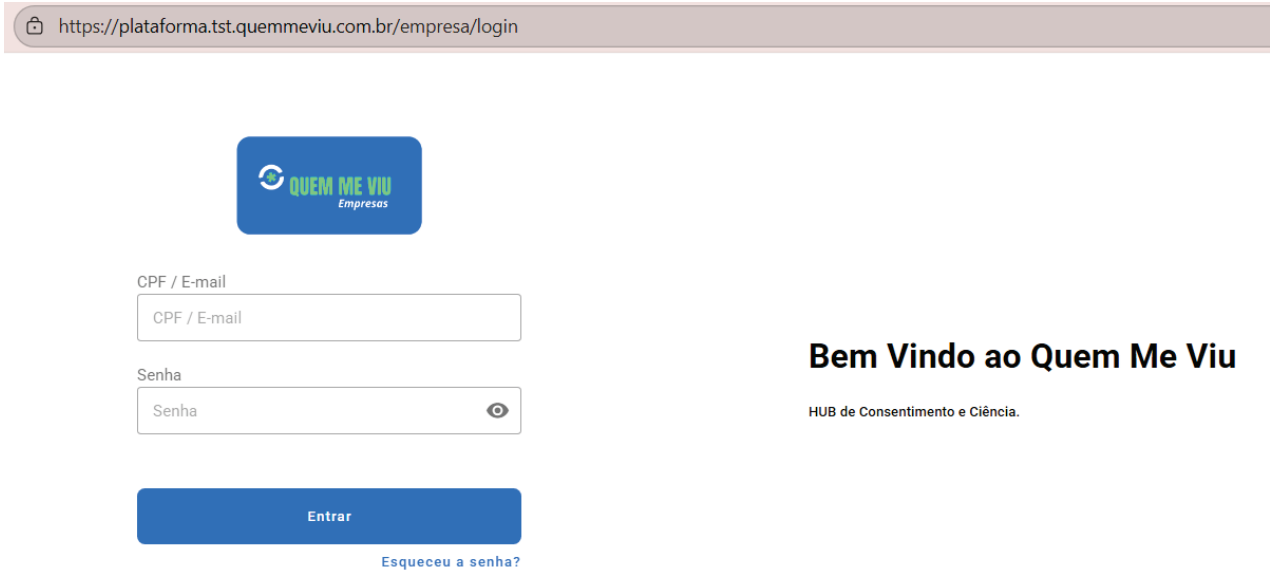
A GCC adota um modelo de controle de acesso baseado em perfis de usuário, garantindo segurança e segregação de funções. Existem quatro tipos principais de usuários:

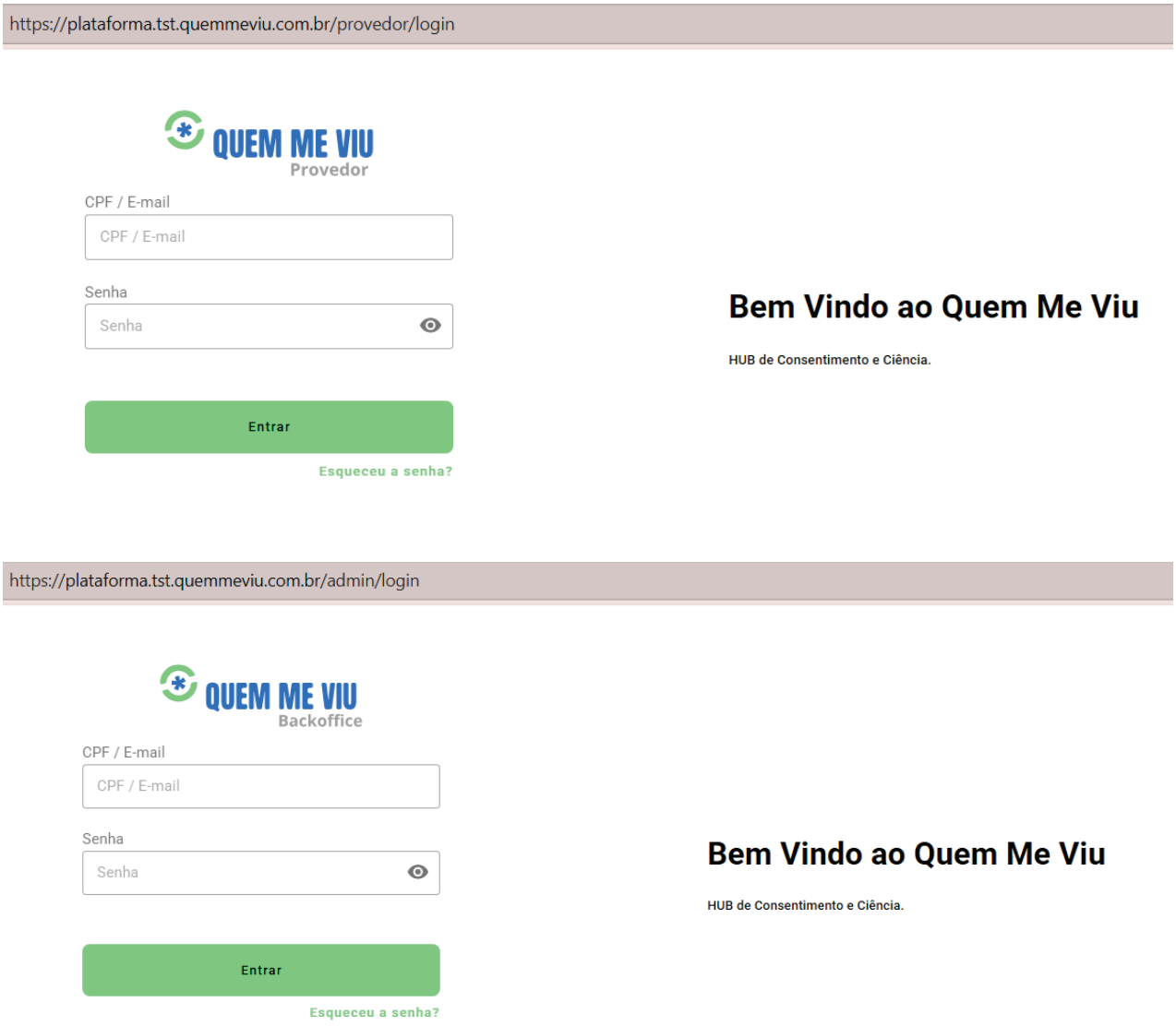
- Backoffice: Responsável por operações internas e gestão administrativa.
- Provedor: Atua no gerenciamento de todo ecossistema da GCC.
- Empresa: Usuários de clientes (empresas). Possui dois subníveis:
  - Administrador: Pode gerenciar a conta da empresa, cadastrar novos usuários e definir permissões.
  - Operacional: Tem acesso apenas para consulta dos usuários cadastrados na empresa, sem permissões de edição ou cadastro de novos usuários.
- Titular: Usuário final que acessa informações relacionadas aos seus próprios dados.

Esse modelo assegura autenticação segura, controle granular de permissões e rastreabilidade das ações, garantindo conformidade com normas de segurança e LGPD.

Prints das plataformas:

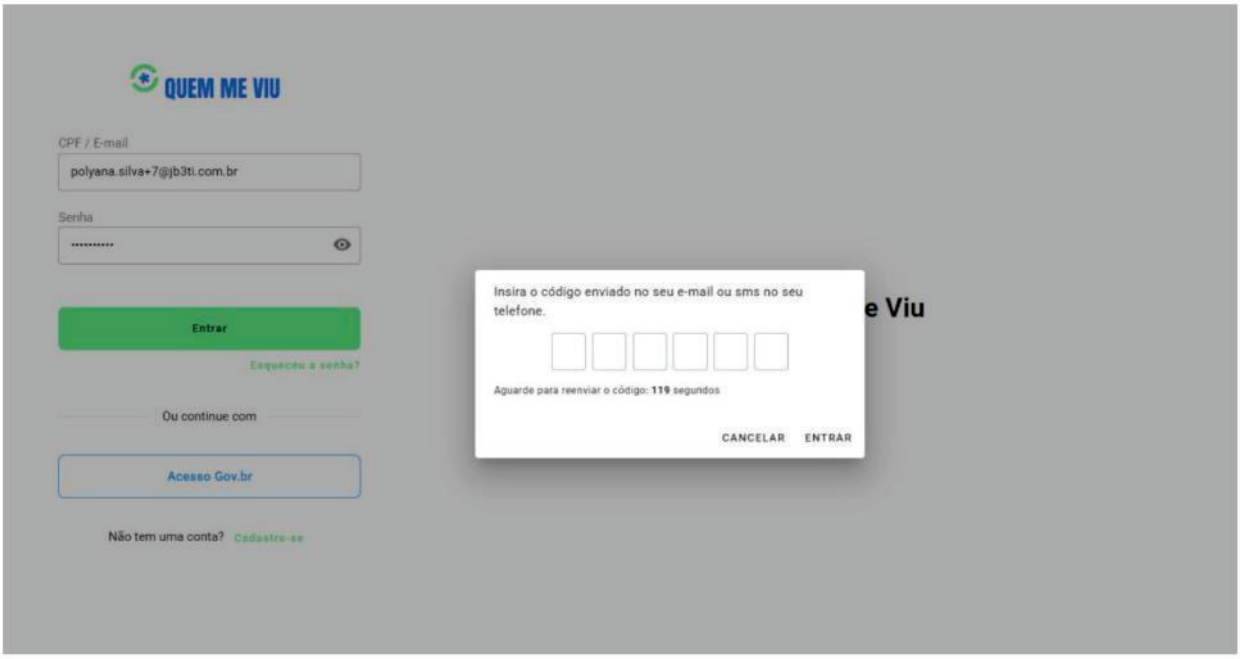

https://plataforma.tst.quemmeviu.com.br/titular/login
QUEM ME VIU
CPF / E-mail
CPF / E-mail
Senha
Senha
Entrar
Esqueceu a senha?
Ou continue com
Acesso Gov.br
Entrar com Certificado
Não tem uma conta? Cadastre-se
Bem Vindo ao Quem Me Viu
HUB de Consentimento e Ciência.


https://plataforma.tst.quemmeviu.com.br/empresa/login
QUEM ME VIU
Empresas
CPF / E-mail
CPF / E-mail
Senha
Senha
Entrar
Esqueceu a senha?
Bem Vindo ao Quem Me Viu
HUB de Consentimento e Ciência.

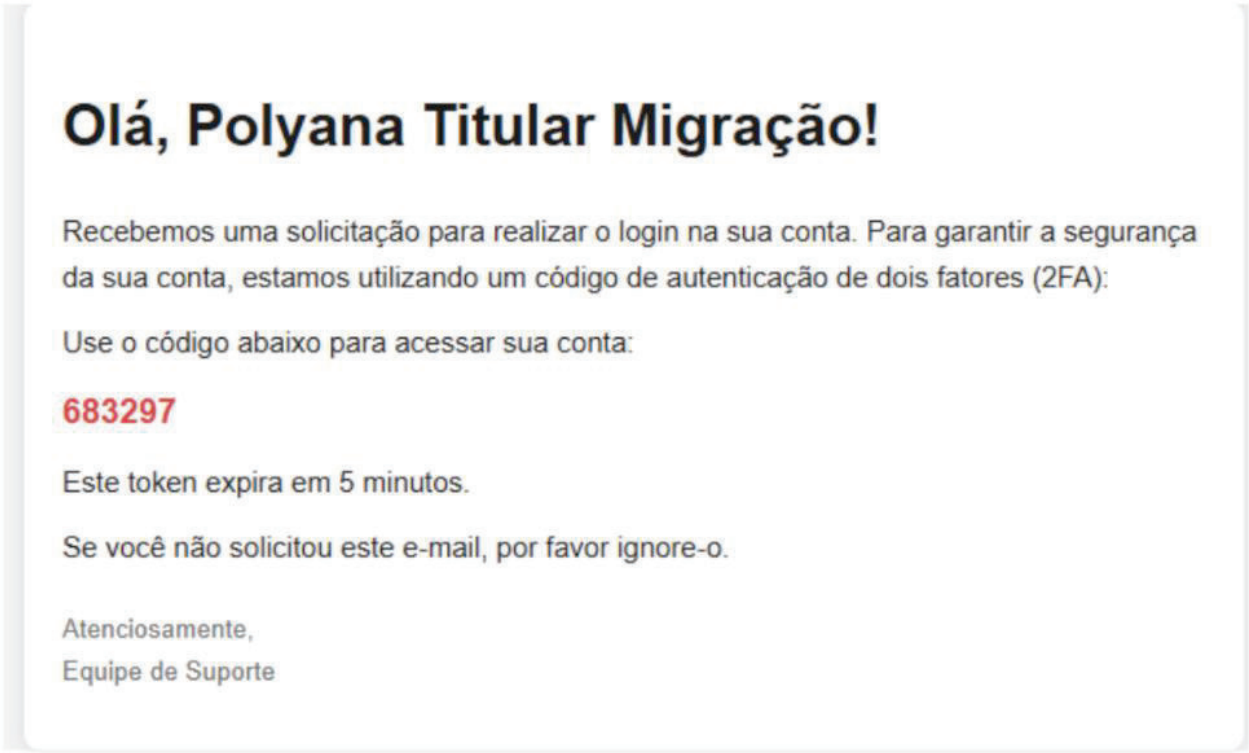


3. Autenticação Segura

O acesso às plataformas da GCC ocorre por meio de autenticação em dois fatores (2FA) para garantir maior segurança. O processo funciona assim:
O usuário informa CPF ou e-mail + senha na tela de login.
É gerado e enviado um token de acesso via SMS e e-mail.
O usuário deve inserir esse código na plataforma para validação.
Somente após a verificação do token, o acesso é liberado.
Esse mecanismo reduz riscos de acesso indevido, garantindo confidencialidade e integridade das informações.



E-mail



Olá, Polyana Titular Migração!

Recebemos uma solicitação para realizar o login na sua conta. Para garantir a segurança da sua conta, estamos utilizando um código de autenticação de dois fatores (2FA):

Use o código abaixo para acessar sua conta:

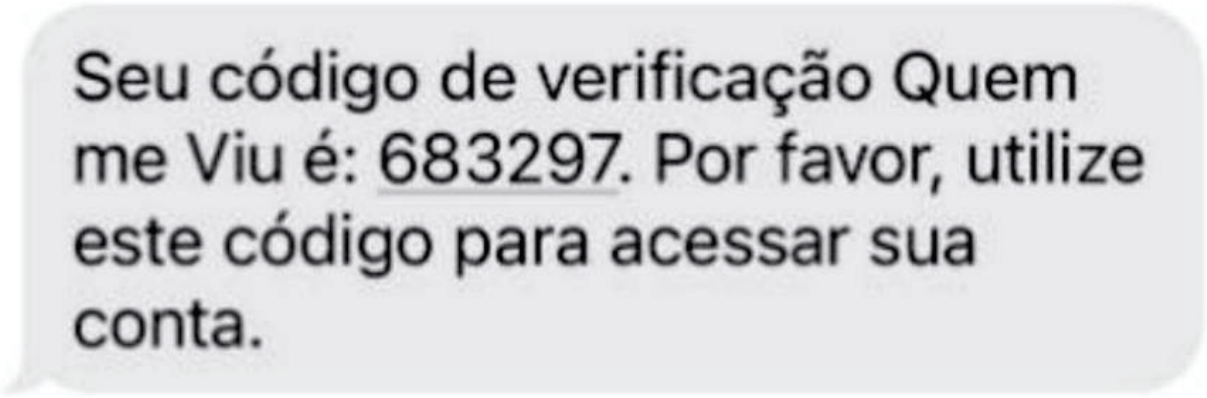
683297

Este token expira em 5 minutos.

Se você não solicitou este e-mail, por favor ignore-o.

Atenciosamente,
Equipe de Suporte

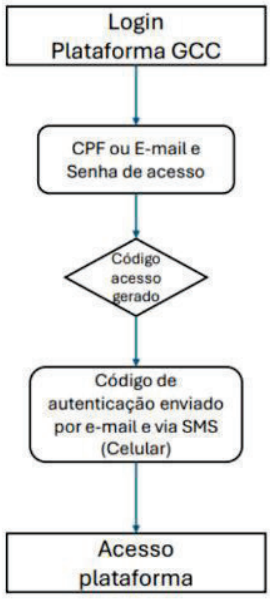
SMS



4. Diagrama de fluxo de autenticação

QUEM ME VIU

Diagrama fluxo autenticação



5. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

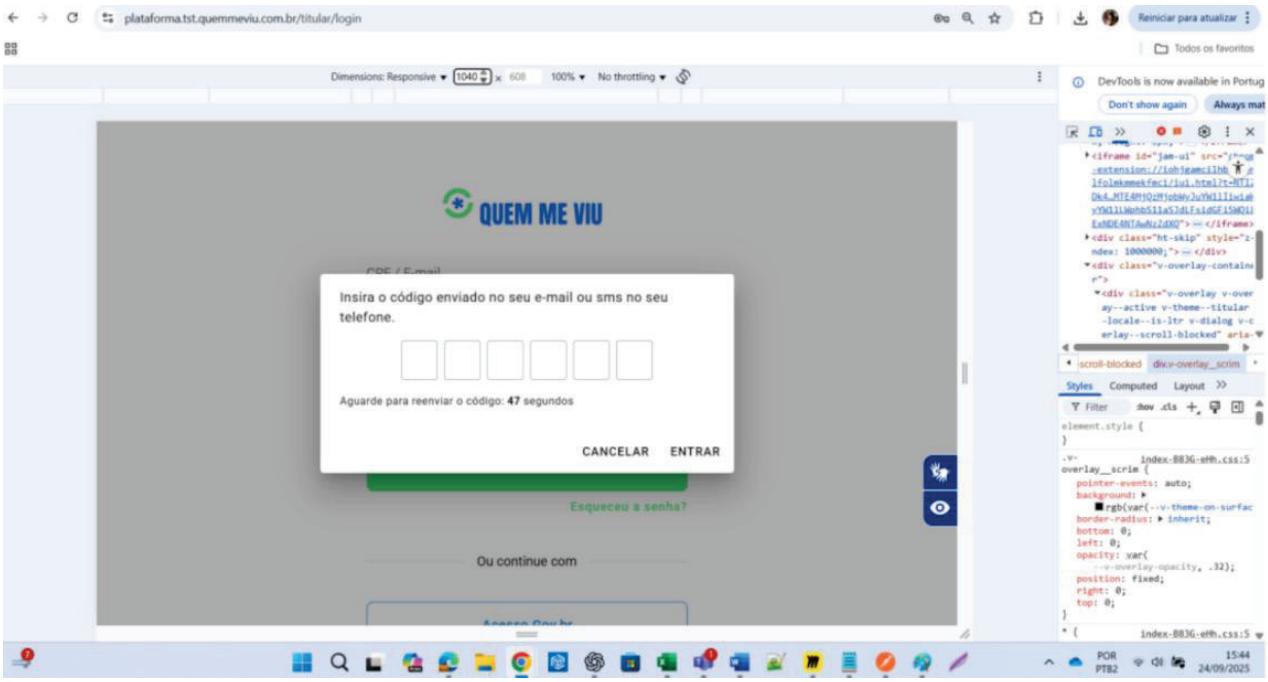
1. Descrição

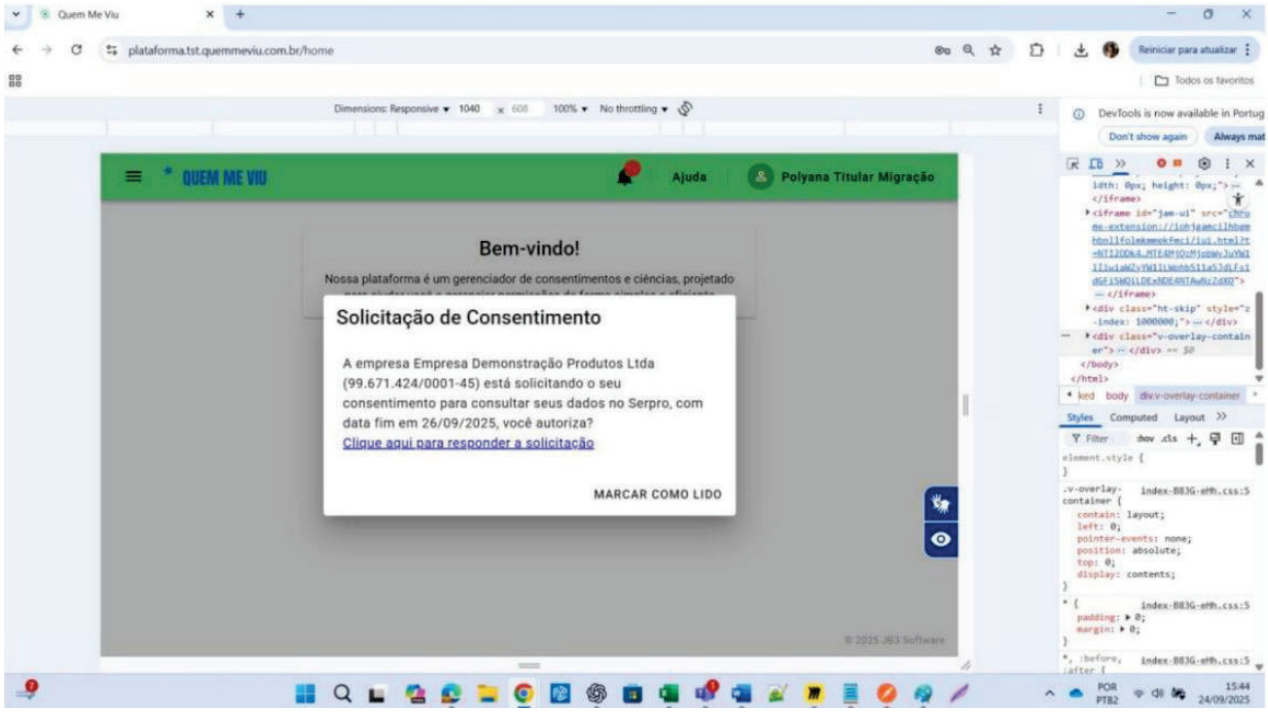
As aplicações foram desenvolvidas de forma web responsivas e mobile (iOS e Android), garantindo interfaces intuitivas, amigáveis e adaptáveis a diferentes dispositivos e tamanhos de tela. As soluções apresentam alta qualidade de UI/UX, priorizando a experiência do usuário, navegabilidade e estética. Além disso, estão em conformidade com os padrões de acessibilidade digital definidos pela WCAG 2.1, assegurando que pessoas com diferentes necessidades possam utilizar as aplicações de forma inclusiva e eficiente.

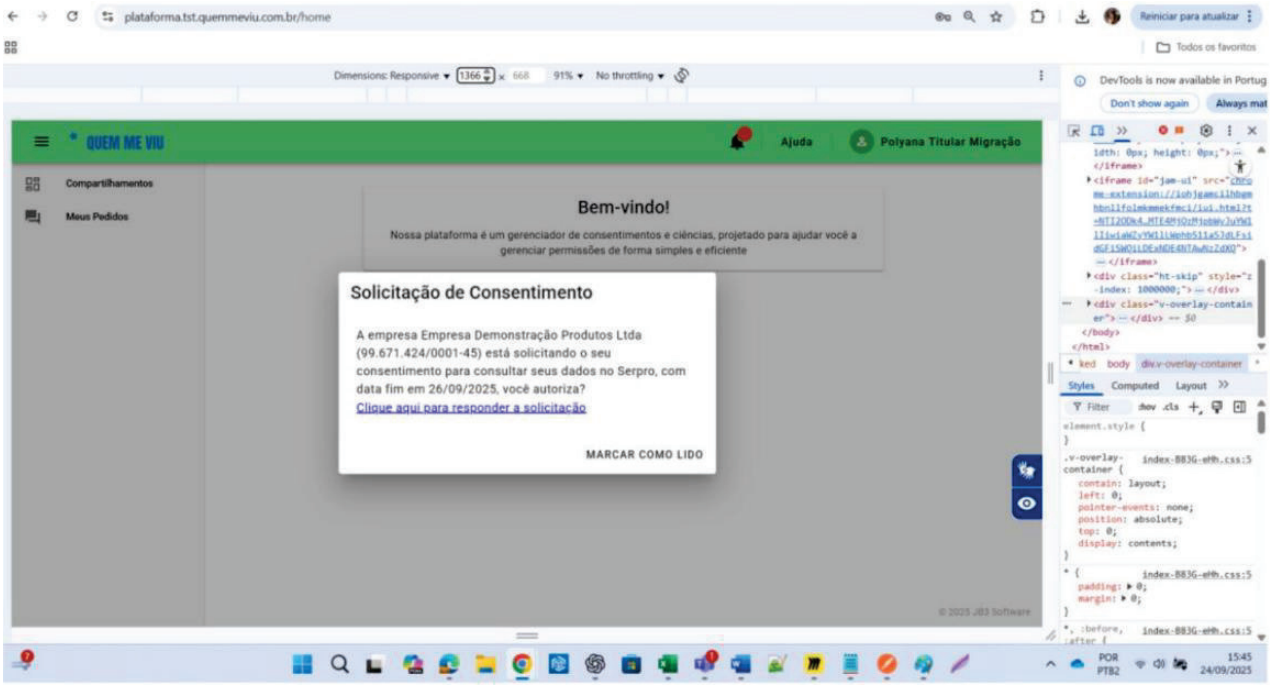
2. Responsividade

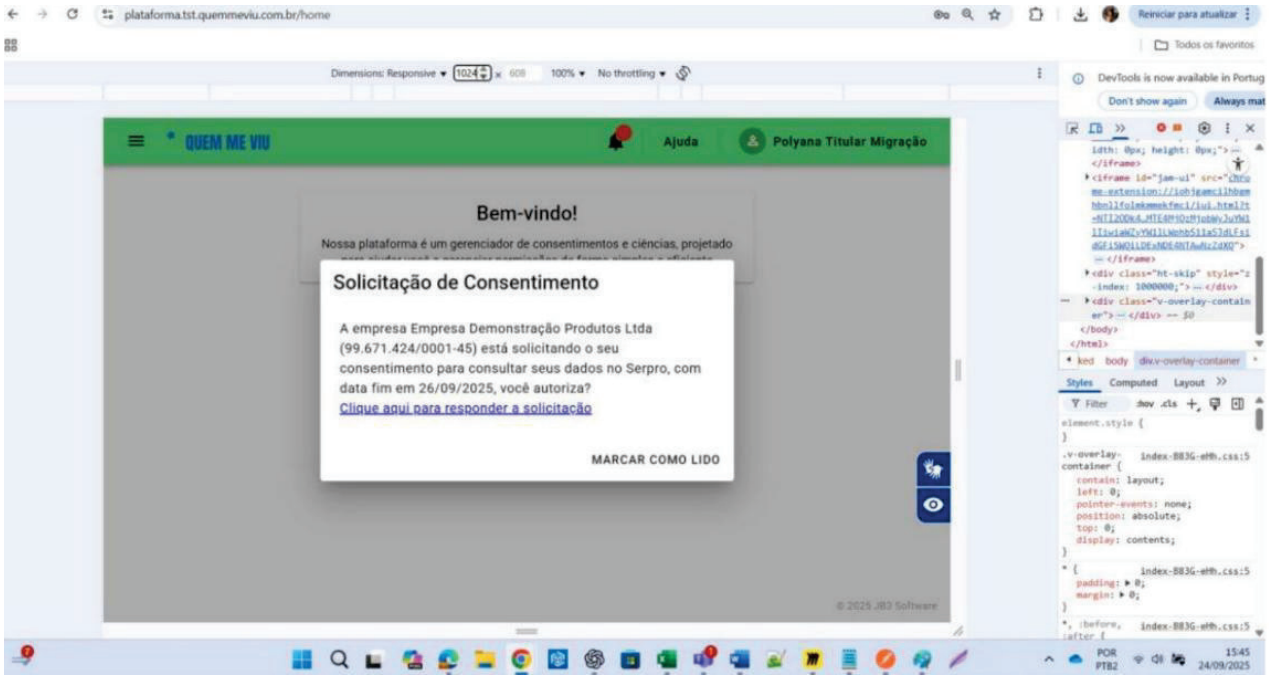
O objetivo da responsividade para desktop, smartphones e tablets visa garantir que as aplicações:
• Adapte-se automaticamente ao tamanho e orientação da tela, mantendo a legibilidade e funcionalidade em qualquer dispositivo.
• Proporcione uma experiência consistente e intuitiva, sem necessidade de zoom ou rolagem excessiva.
• Otimize a usabilidade e a estética, ajustando elementos como menus, botões, imagens e textos para diferentes resoluções.
• Melhore a acessibilidade, permitindo que usuários com diferentes dispositivos e condições de conexão tenham acesso eficiente ao conteúdo.
• Aumente a performance e engajamento, já que interfaces responsivas reduzem fricções e tornam a navegação mais agradável.

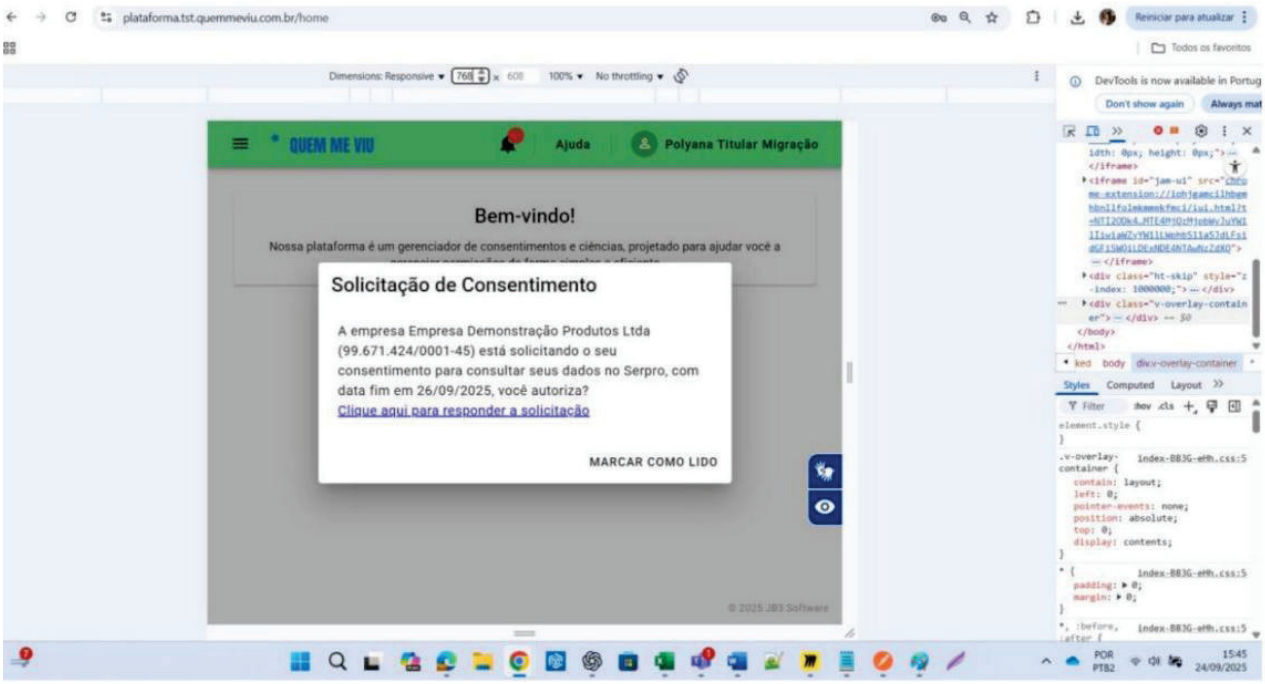
Breakpoints:
• 1440px (desktop widescreen)
• 1366px (desktop padrão)
• 1024px (tablet landscape)
• 768px (tablet portrait)
• 480px (smartphones médios)
• 320px (smartphones pequenos)

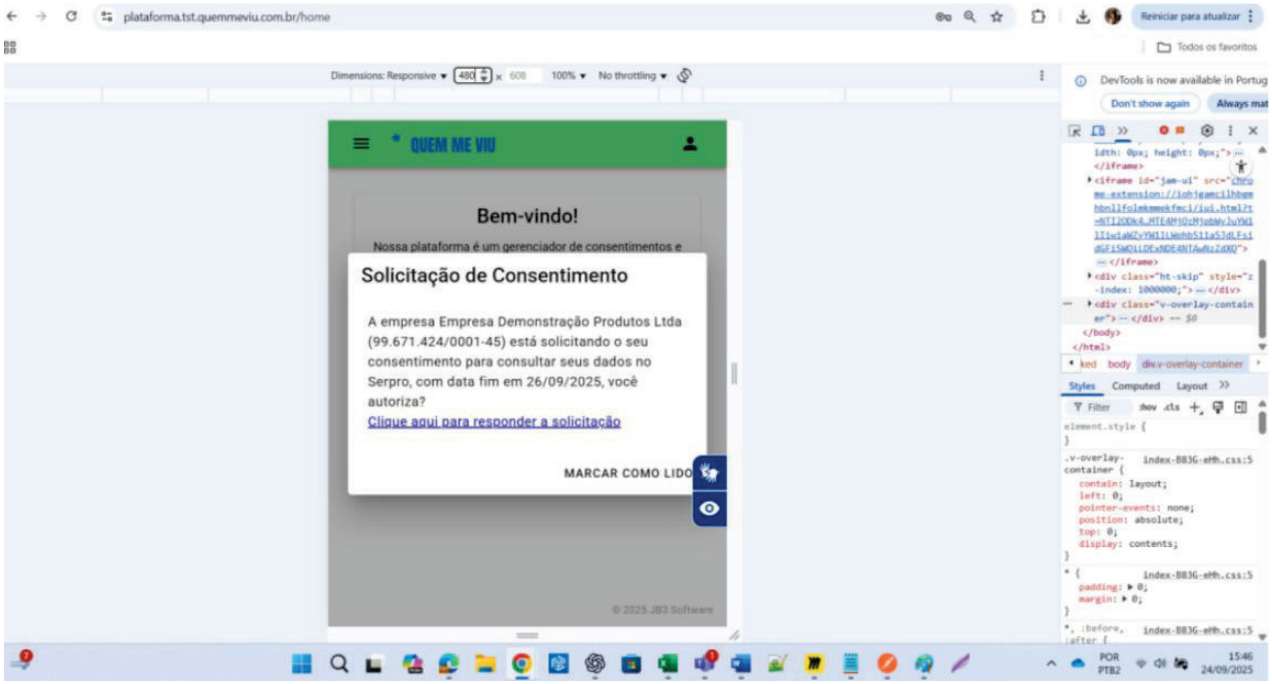

plataforma.tst.quemmeviu.com.br/titular/login
QUEM ME VIU
Insira o código enviado no seu e-mail ou sms no seu telefone.
Aguarde para reenviar o código: 47 segundos
CANCELAR
ENTRAR
Esqueceu a senha?
Ou continue com

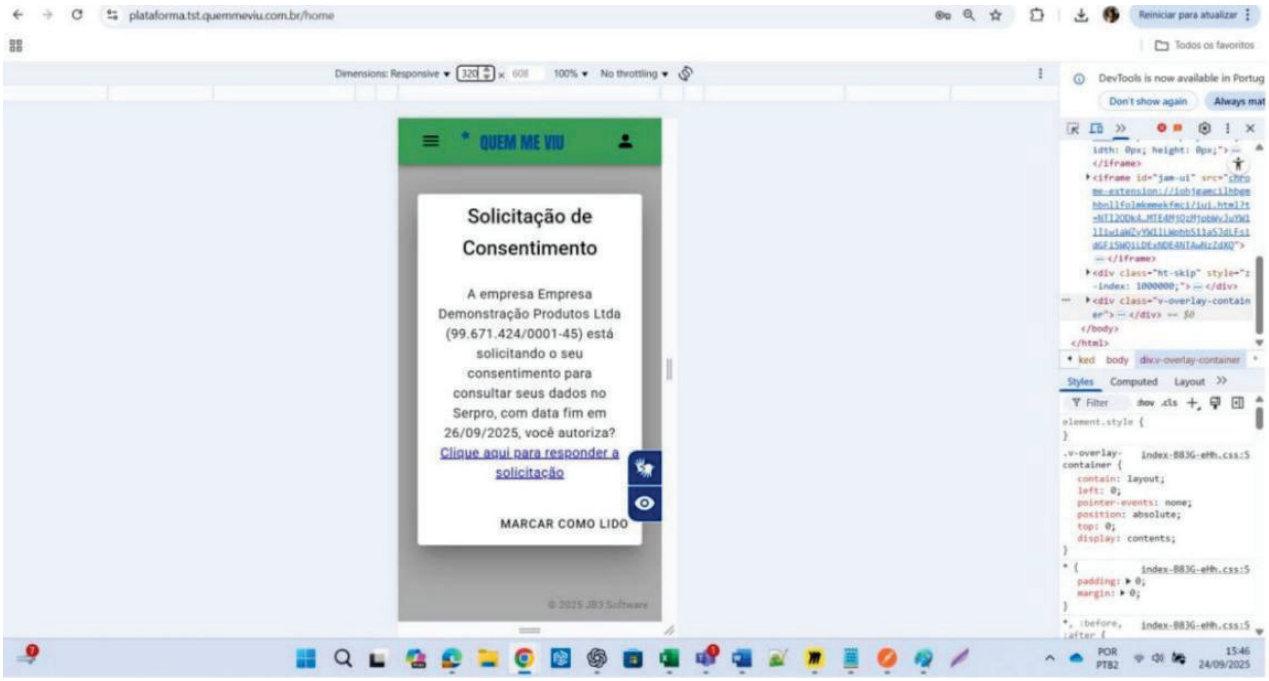

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Polyana Titular Migração
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO

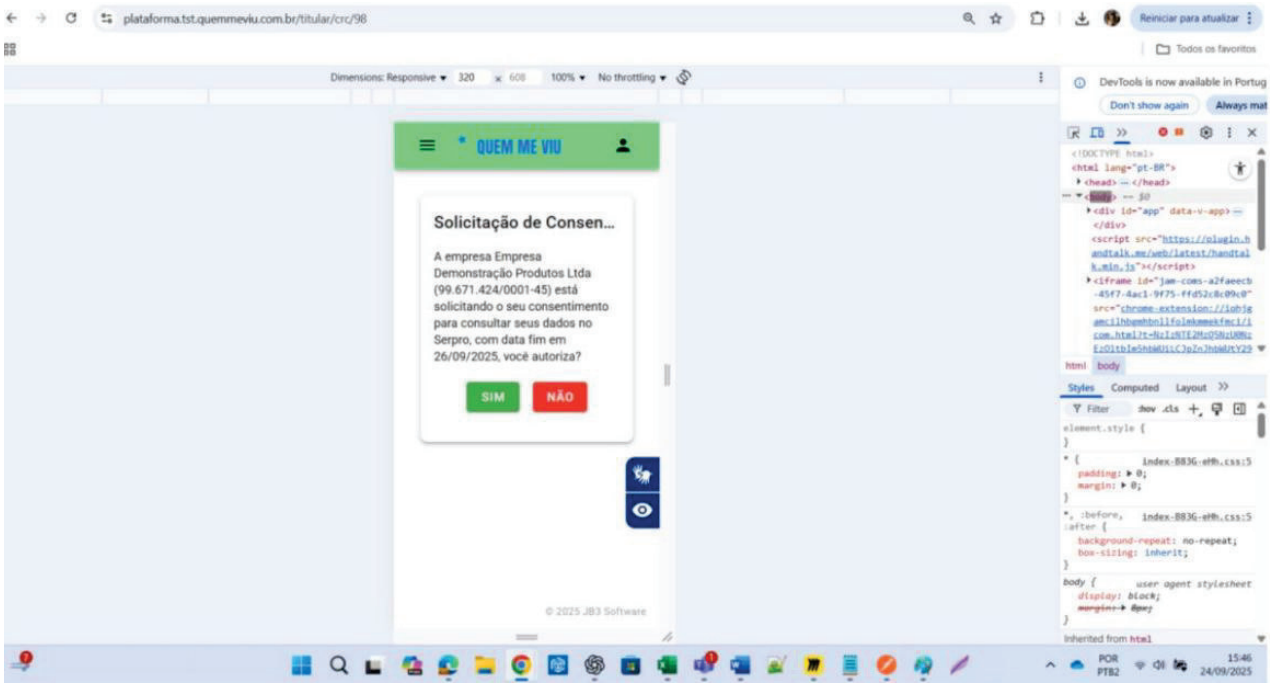

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Polyana Titular Migração
Compartilhamentos
Meus Pedidos
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO

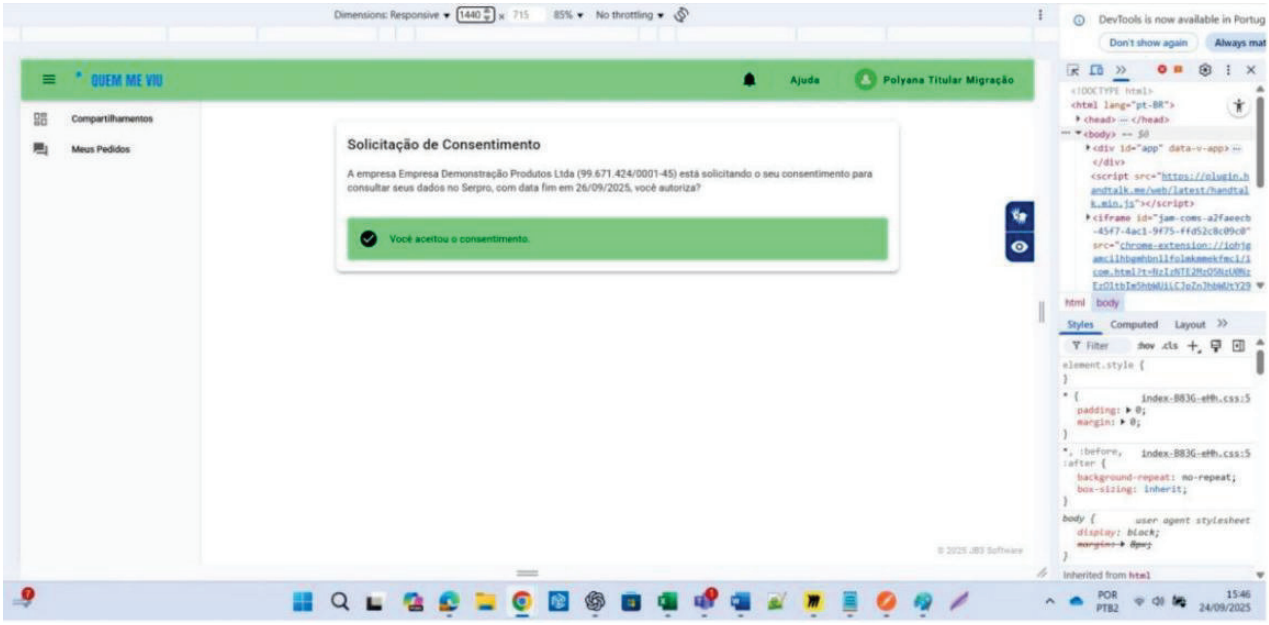

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Polyana Titular Migração
Bem-vindo!
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO

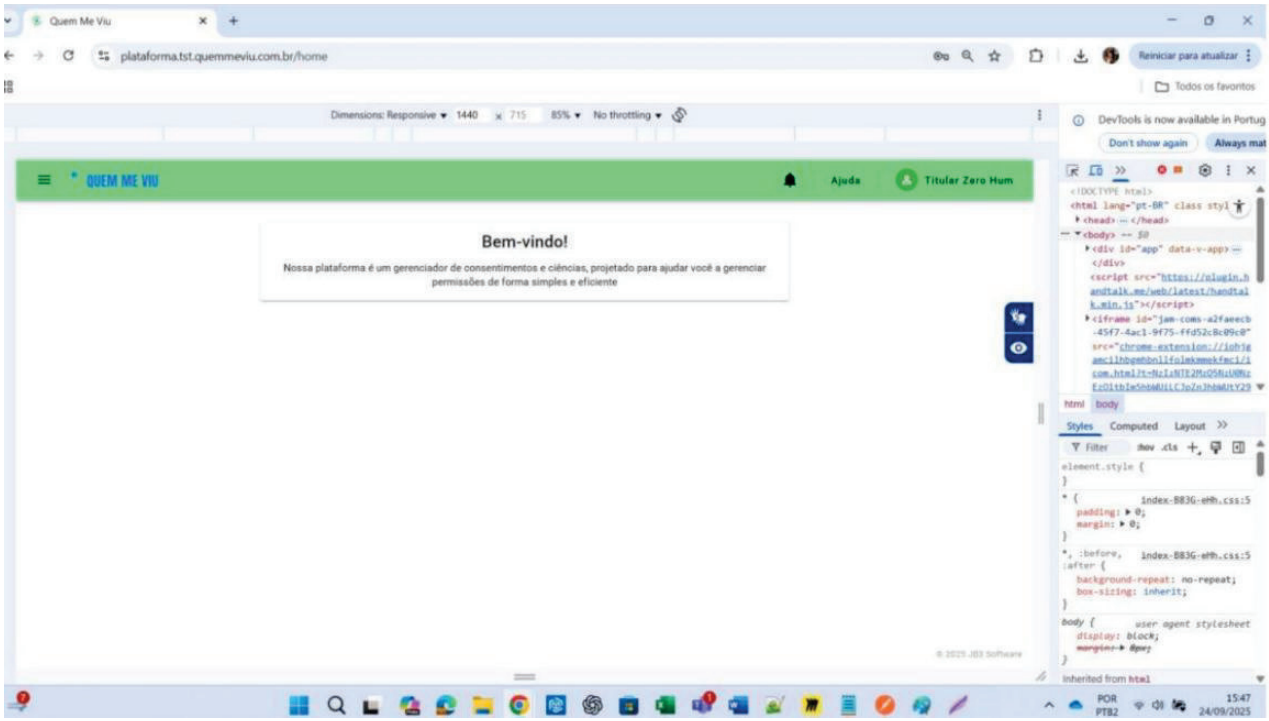

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Polyana Titular Migração
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO
© 2025 JB3 Software

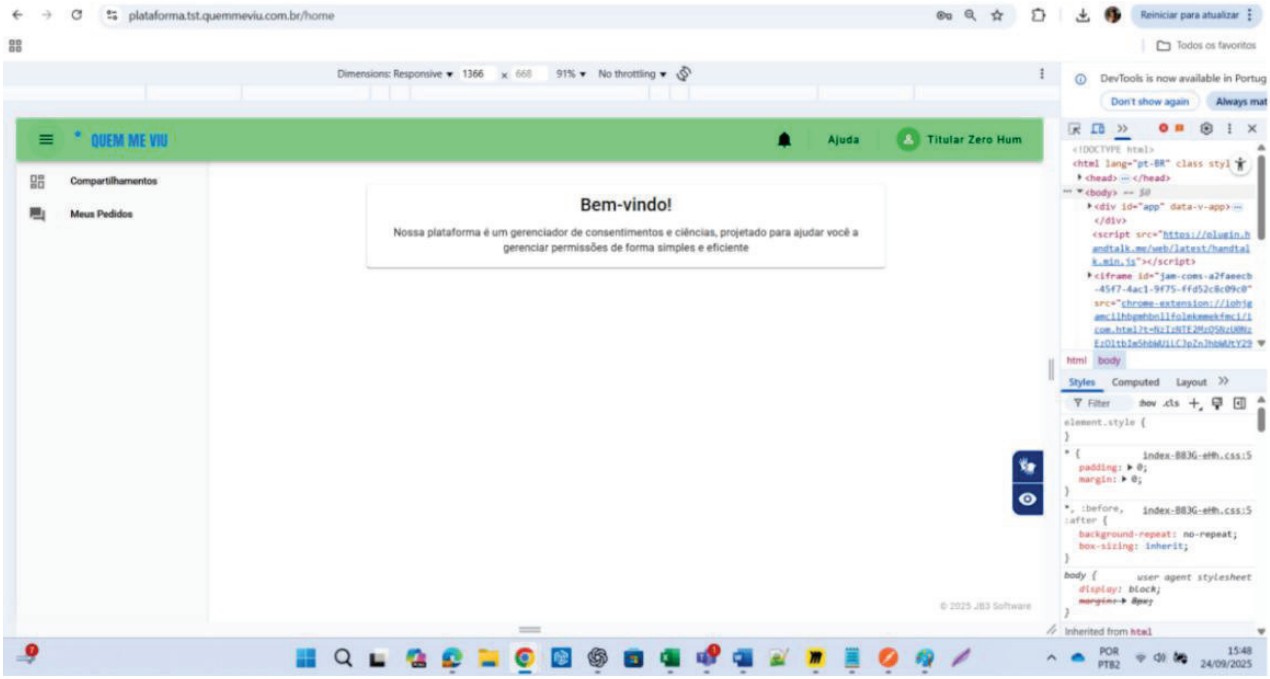

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO
© 2025 JB3 Software

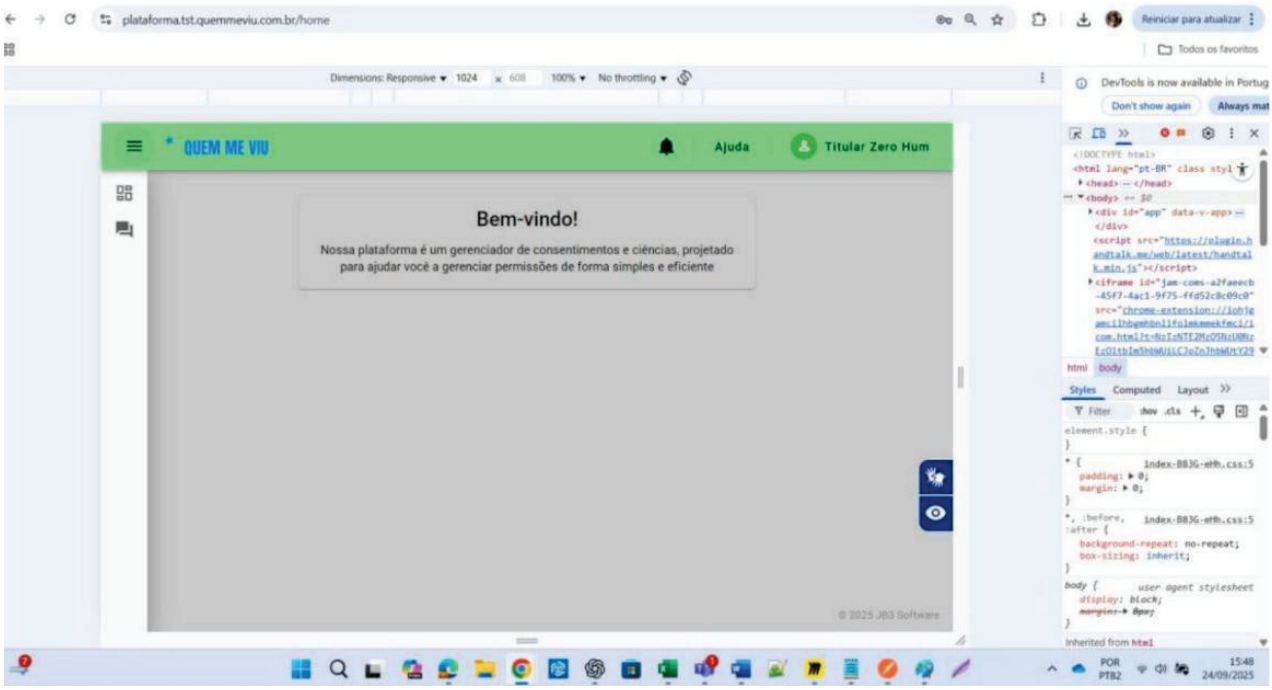

plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Clique aqui para responder a solicitação
MARCAR COMO LIDO
© 2025 JB3 Software

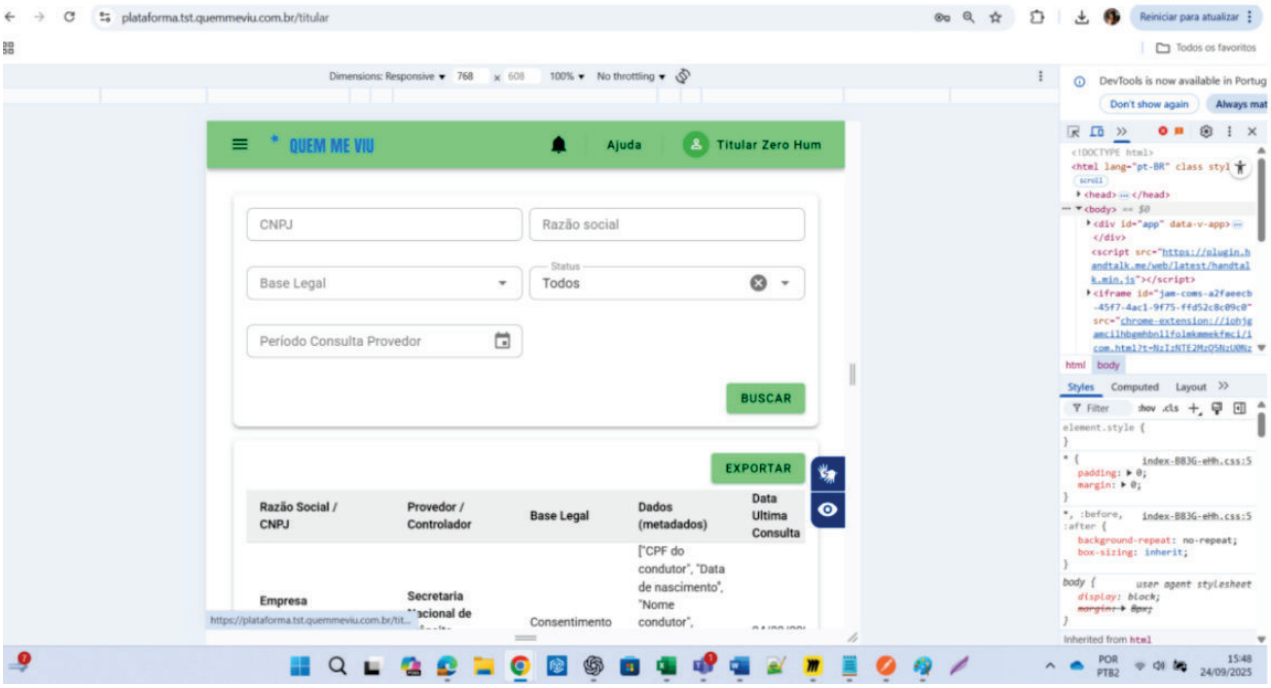

plataforma.tst.quemmeviu.com.br/titular/crc/98
QUEM ME VIU
Solicitação de Consen...
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
SIM
NÃO
© 2025 JB3 Software

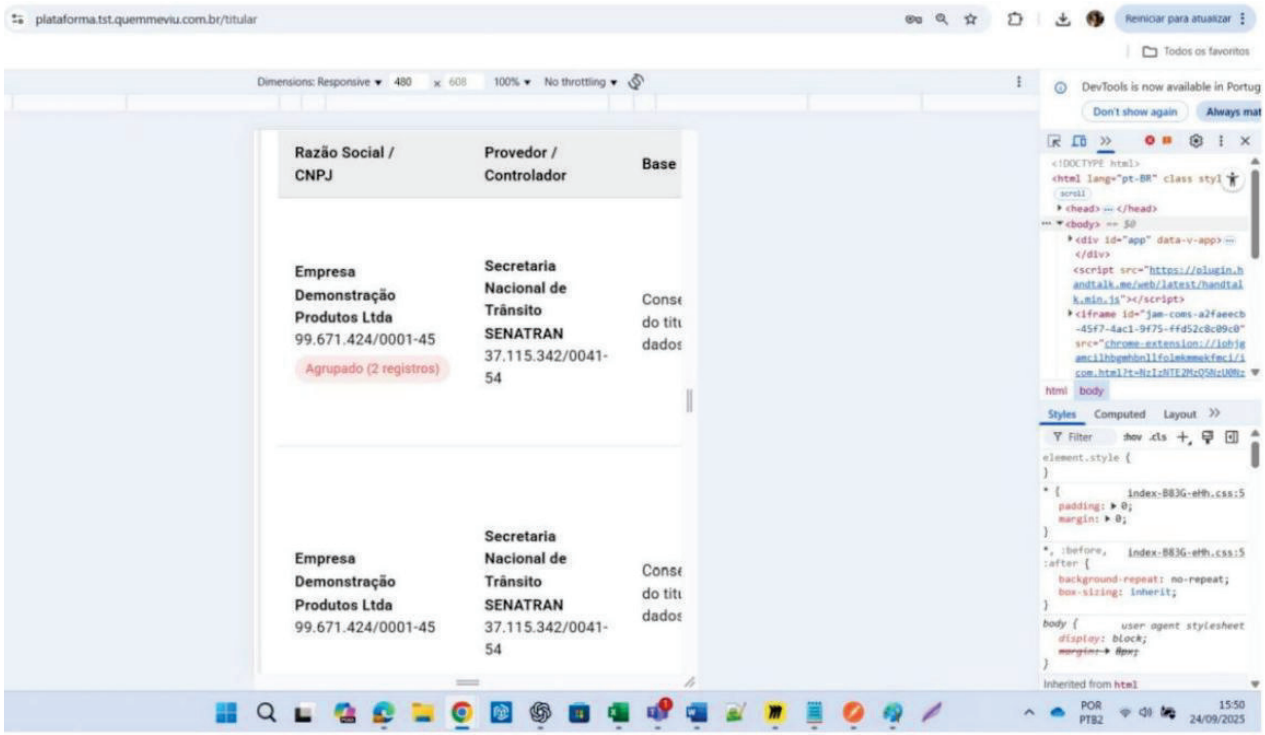

QUEM ME VIU
Ajuda
Polyana Titular Migração
Compartilhamentos
Meus Pedidos
Solicitação de Consentimento
A empresa Empresa Demonstração Produtos Ltda (99.671.424/0001-45) está solicitando o seu consentimento para consultar seus dados no Serpro, com data fim em 26/09/2025, você autoriza?
Você aceitou o consentimento.

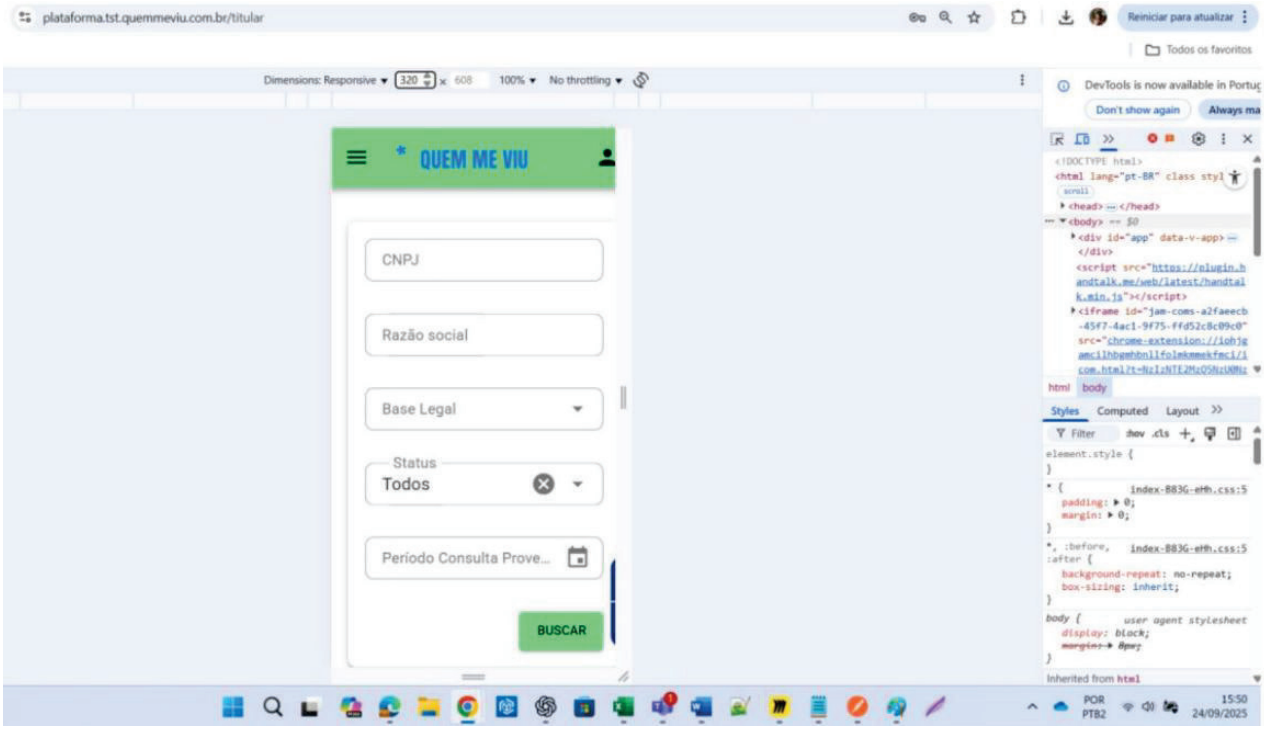

Quem Me Viu
plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Zero Hum
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente


plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Zero Hum
Compartilhamentos
Meus Pedidos
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
© 2025 JB3 Software


plataforma.tst.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Zero Hum
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
© 2025 JB3 Software

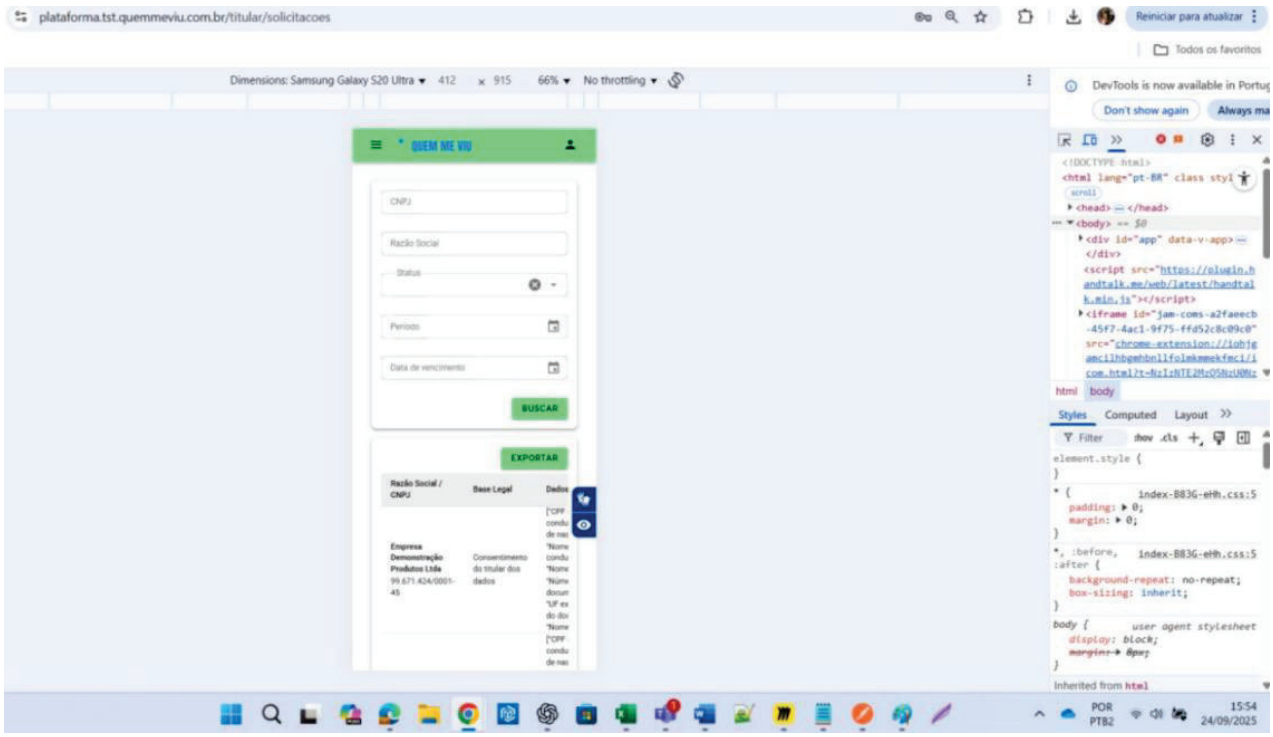

plataforma.tst.quemmeviu.com.br/titular
QUEM ME VIU
Ajuda
Titular Zero Hum
CNPJ
Razão social
Base Legal
Status
Todos
Período Consulta Provedor
BUSCAR
EXPORTAR
Razão Social / CNPJ
Provedor / Controlador
Base Legal
Dados (metadados)
Data Ultima Consulta
Empresa
Secretaria
Consentimento
["CPF do condutor", "Data de nascimento", "Nome condutor",

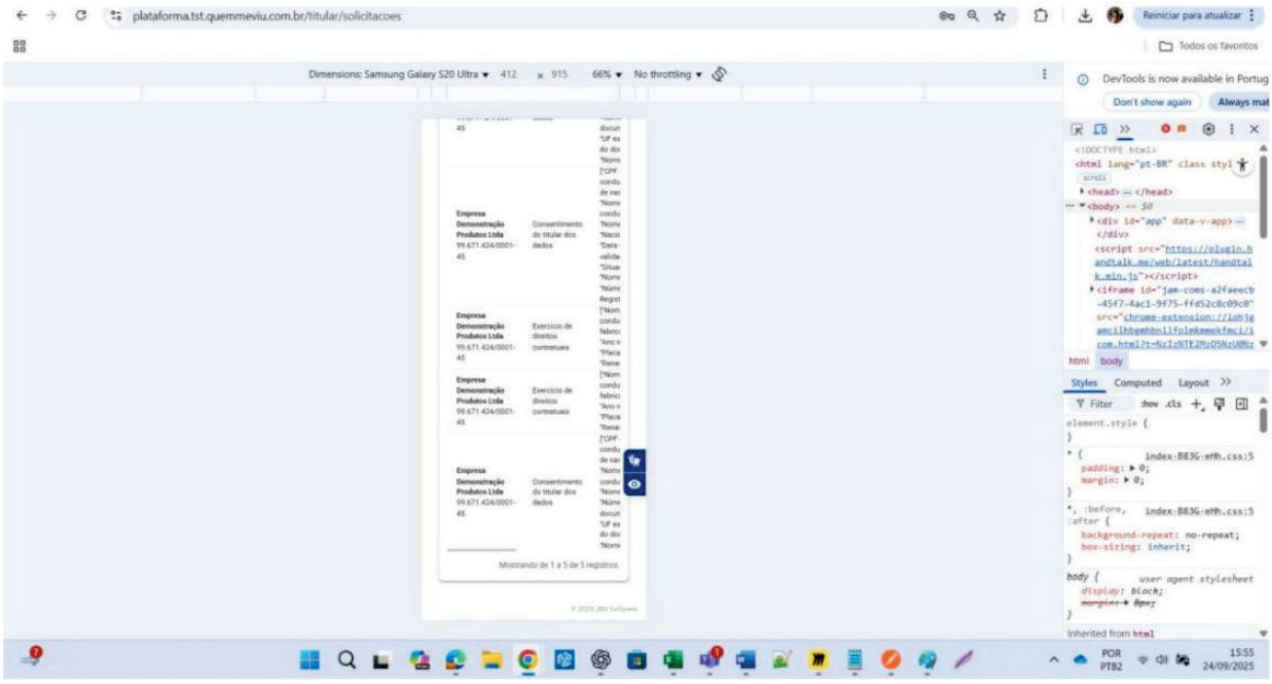

plataforma.tst.quemmeviu.com.br/titular
Razão Social / CNPJ
Provedor / Controlador
Base
Empresa Demonstração Produtos Ltda
99.671.424/0001-45
Agrupado (2 registros)
Secretaria Nacional de Trânsito SENATRAN
37.115.342/0041-54
Empresa Demonstração Produtos Ltda
99.671.424/0001-45
Secretaria Nacional de Trânsito SENATRAN
37.115.342/0041-54

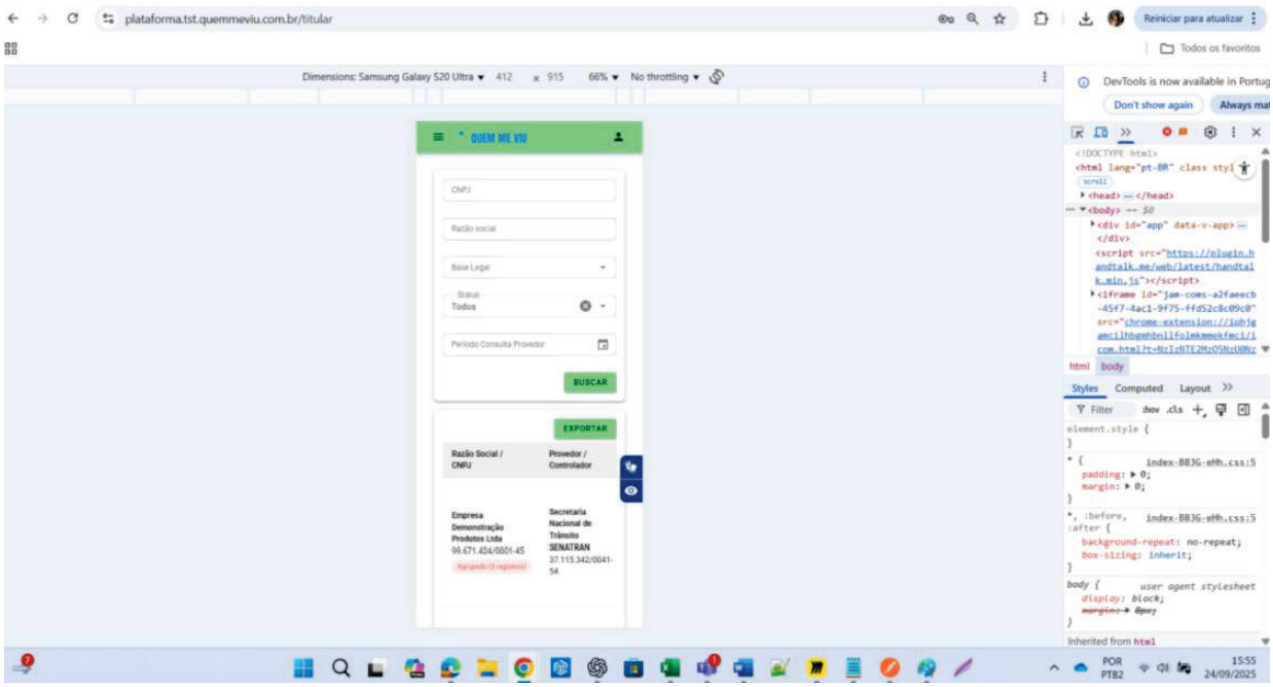


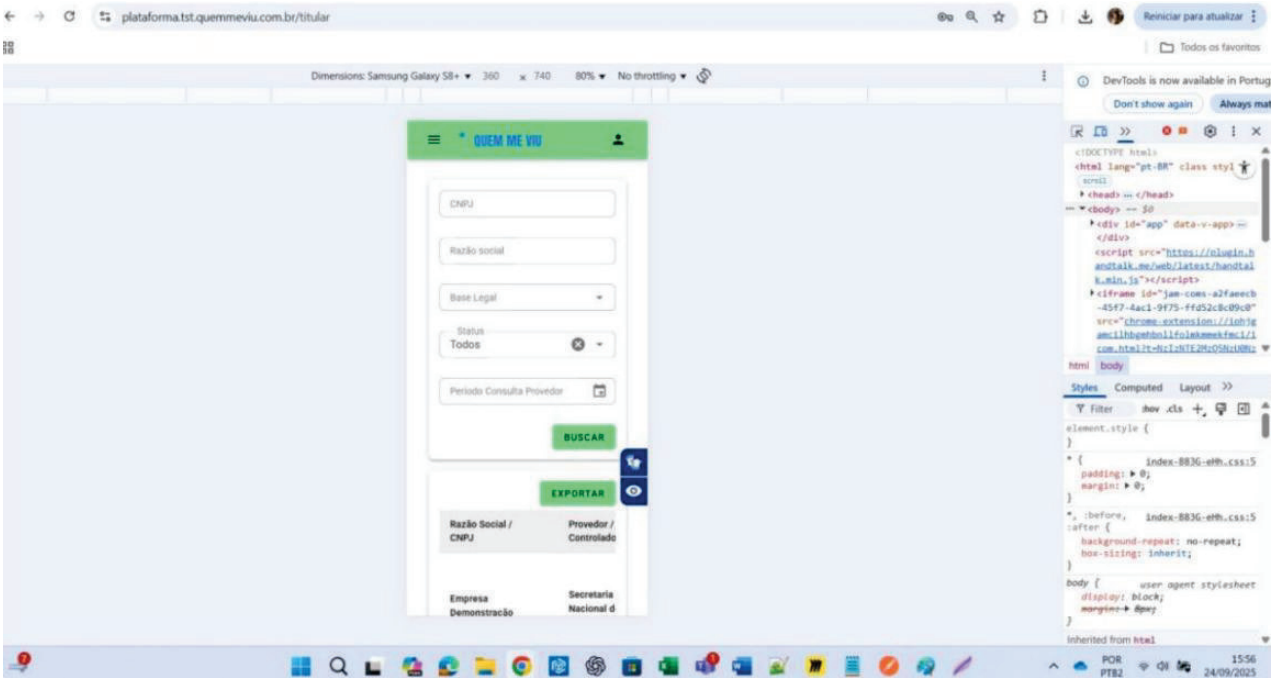
Smartphone

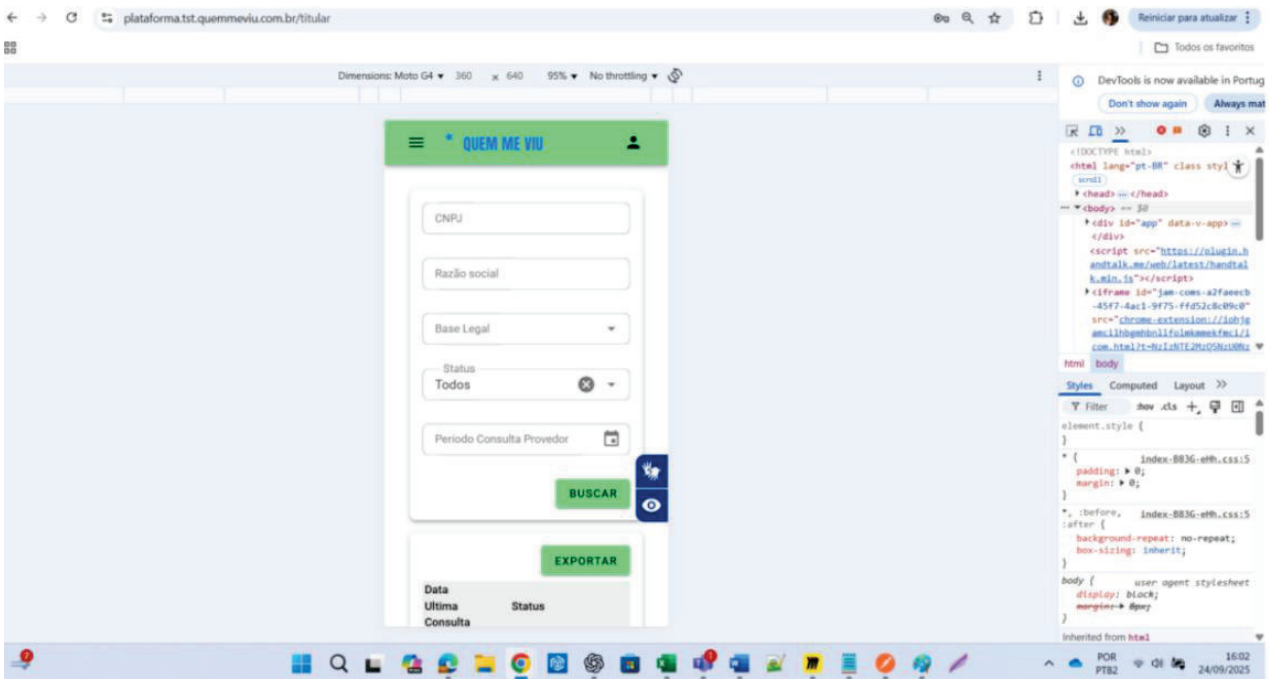
Android

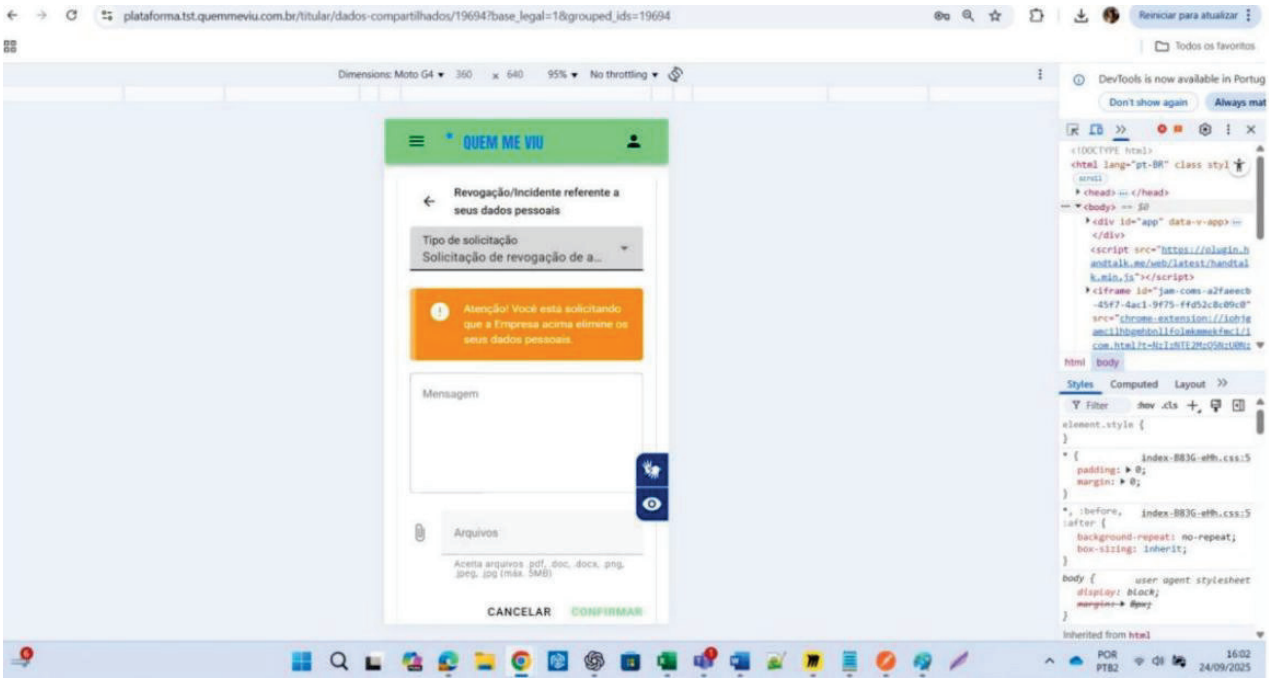



plataforma.tst.quemmeviu.com.br/titular/solicitacoes
Dimensions: Samsung Galaxy S20 Ultra 412 x 915 66% No throttling
Mostrando de 1 a 5 de 5 registros.

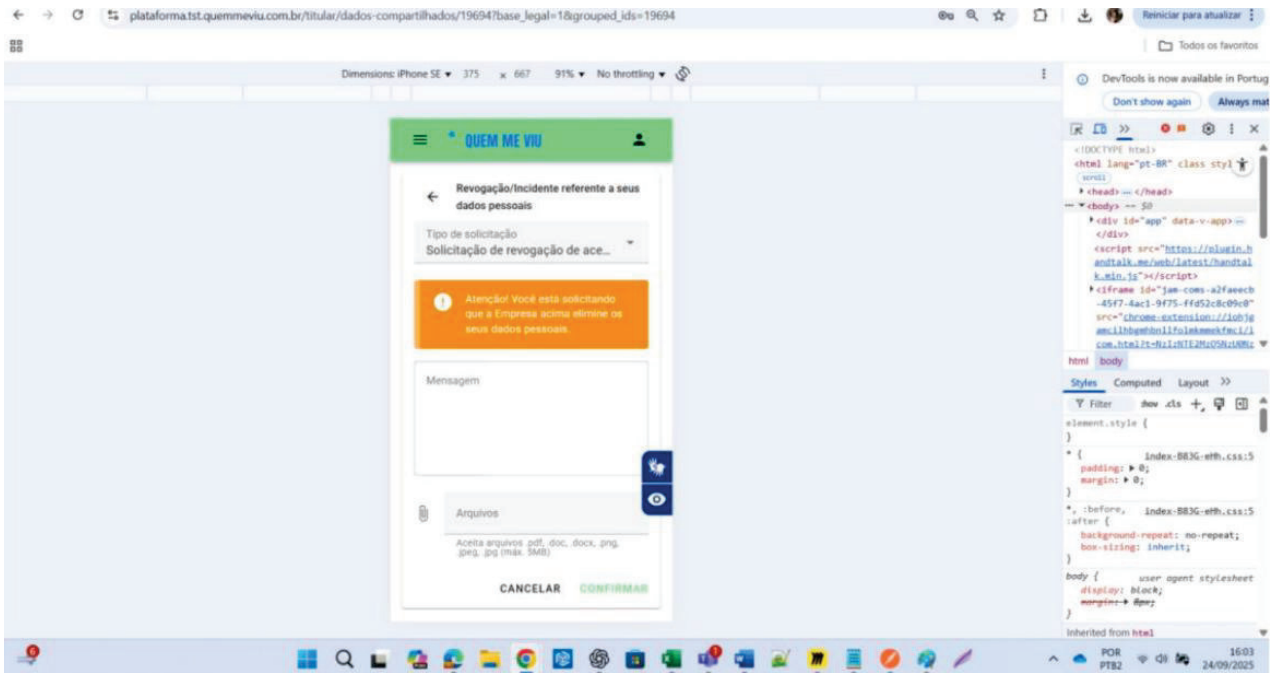

plataforma.tst.quemmeviu.com.br/titular
Dimensions: Samsung Galaxy S20 Ultra 412 x 915 66% No throttling
QUEM ME VIU
CNPJ
Razão social
Base Legal
Status
Todos
Período Consulta Provedor
BUSCAR
EXPORTAR
Razão Social / CNPJ
Provedor / Controlador
Empresa Demonstração Produtos Ltda 99.671.424/0001-45
Secretaria Nacional de Trânsito SENATRAN 37.115.342/0041-54

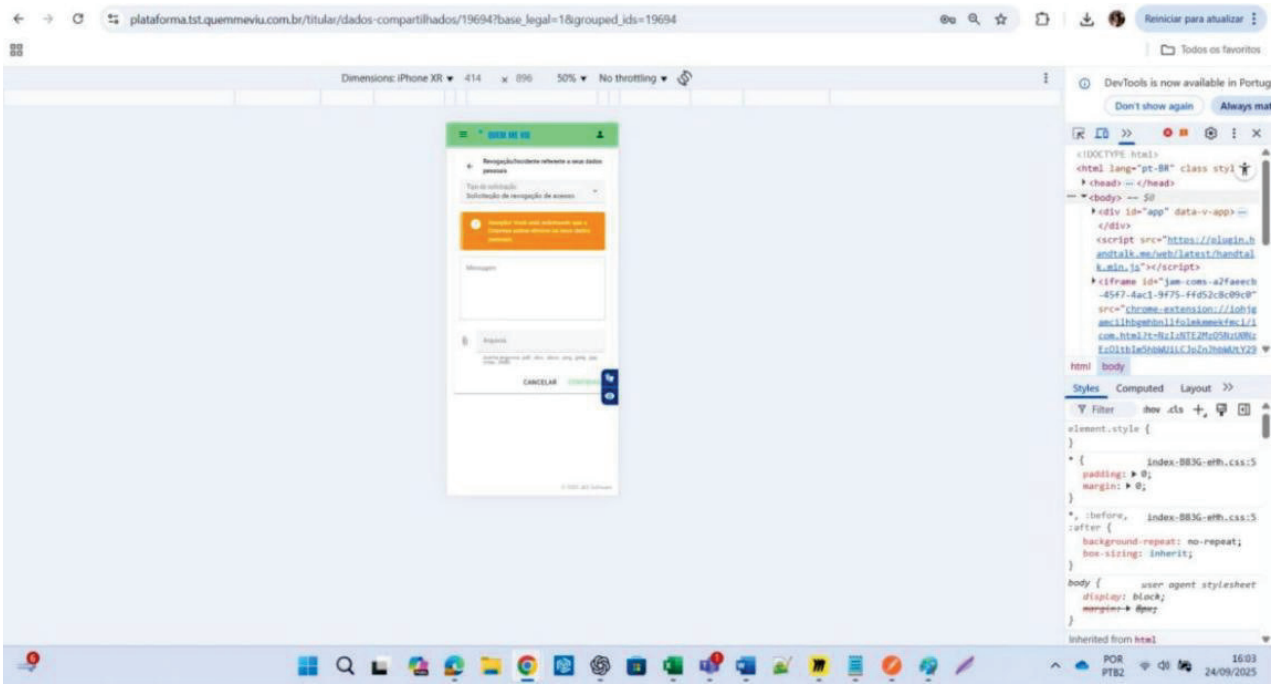

plataforma.tst.quemmeviu.com.br/titular
Reiniciar para atualizar
Dimensions: Samsung Galaxy S8+ 360 x 740 80% No throttling
QUEM ME VIU
CNPJ
Razão social
Base Legal
Status
Todos
Periodo Consulta Provedor
BUSCAR
EXPORTAR
Razão Social / CNPJ
Provedor / Controlado
Empresa Demonstração
Secretaria Nacional d
DevTools is now available in Portug
Don't show again
Always mat
Styles
Computed
Layout
Filter
element.style {
}
* {
padding: ▶ 0;
margin: ▶ 0;
}
*, :before, :after {
background-repeat: no-repeat;
box-sizing: inherit;
}
body {
display: block;
}
Inherited from html
POR PTB2
15:56
24/09/2025

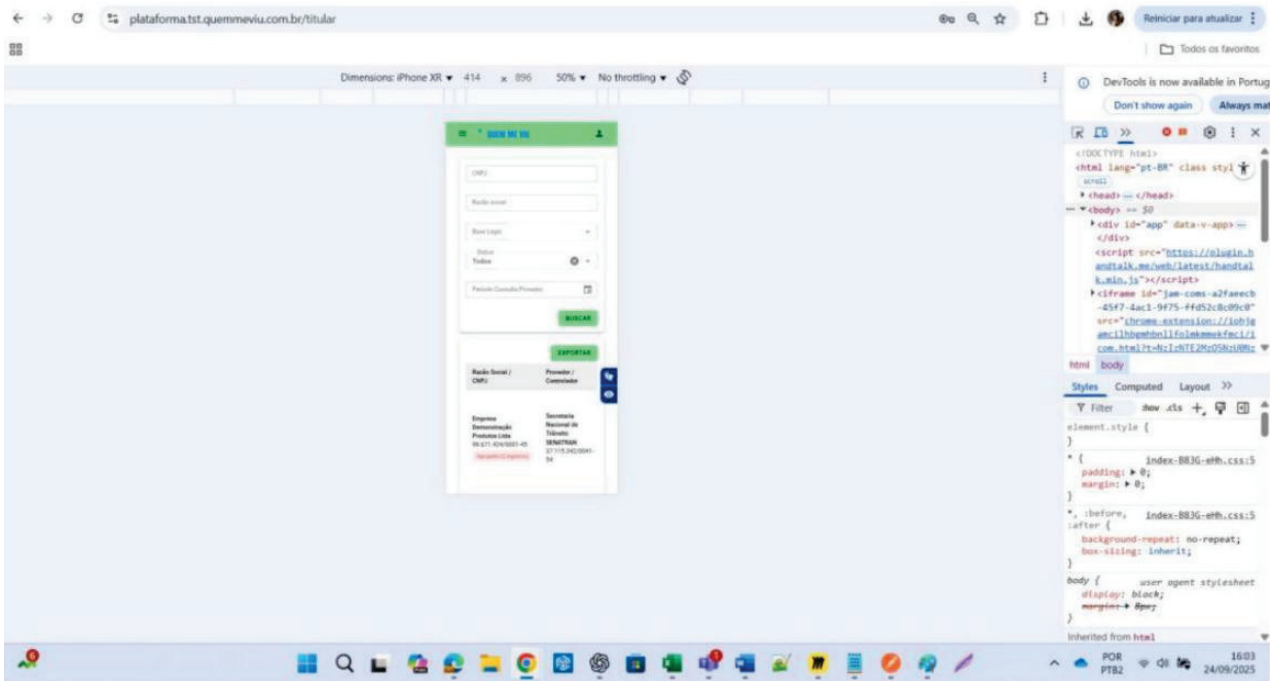

plataforma.tst.quemmeviu.com.br/titular
Reiniciar para atualizar
Dimensions: Moto G4 360 x 640 95% No throttling
QUEM ME VIU
CNPJ
Razão social
Base Legal
Status
Todos
Periodo Consulta Provedor
BUSCAR
EXPORTAR
Data Ultima Consulta
Status
DevTools is now available in Portug
Don't show again
Always mat
Styles
Computed
Layout
Filter
element.style {
}
* {
padding: ▶ 0;
margin: ▶ 0;
}
*, :before, :after {
background-repeat: no-repeat;
box-sizing: inherit;
}
body {
display: block;
}
Inherited from html
POR PTB2
16:02
24/09/2025

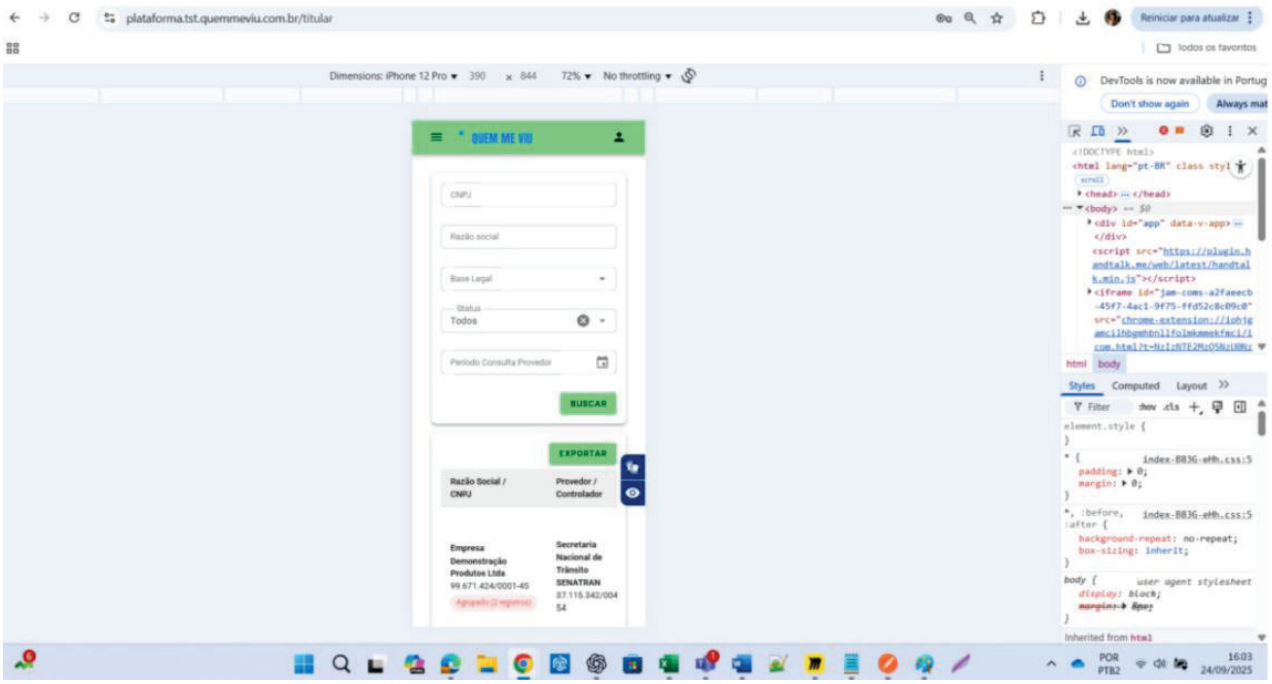

QUEM ME VIU
Revogação/Incidente referente a seus dados pessoais
Tipo de solicitação
Solicitação de revogação de a...
Atenção! Você está solicitando que a Empresa acima elimine os seus dados pessoais.
Mensagem
Arquivos
CANCELAR
CONFIRMAR

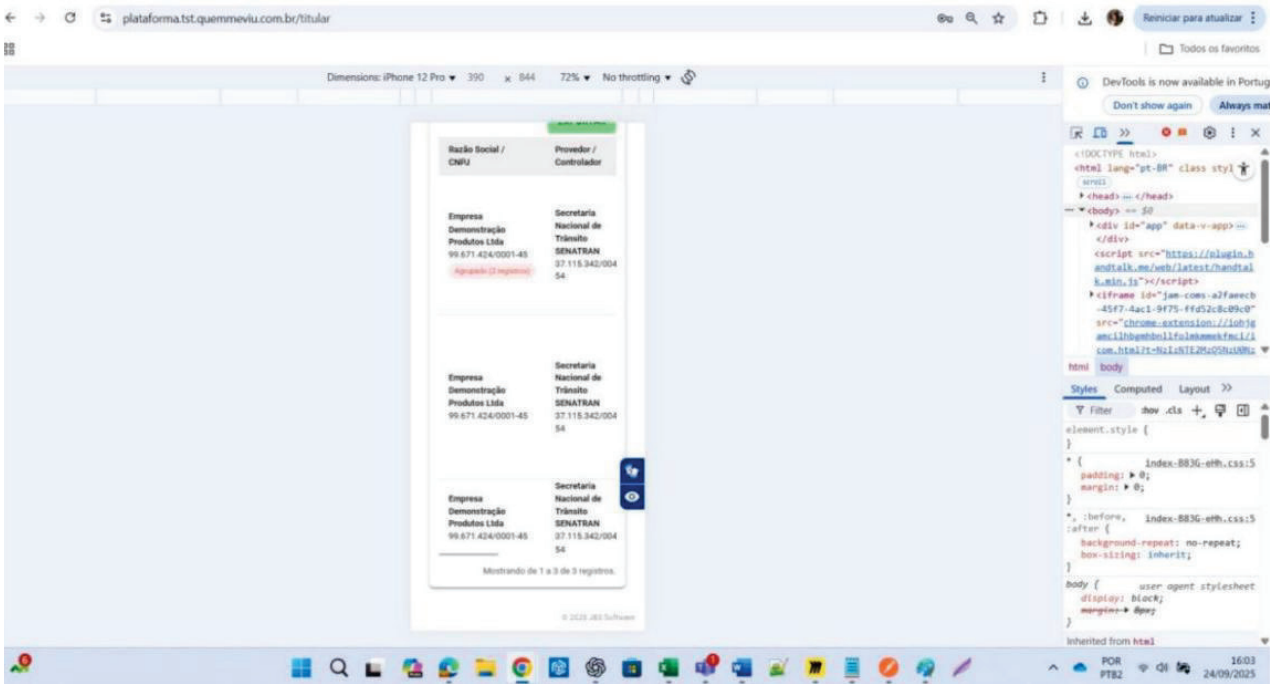
IOS


QUEM ME VIU
Revogação/Incidente referente a seus dados pessoais
Tipo de solicitação
Solicitação de revogação de ace...
Atenção! Você está solicitando que a Empresa acima elimine os seus dados pessoais.
Mensagem
Arquivos
CANCELAR
CONFIRMAR

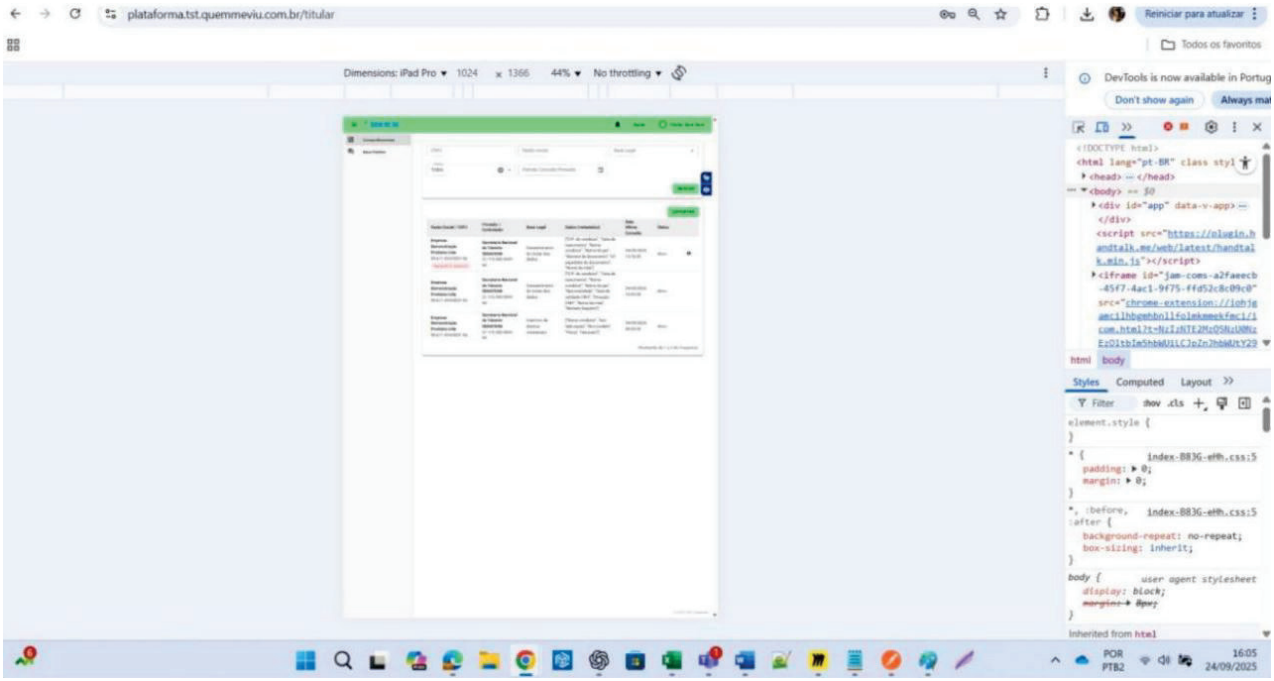

plataforma.tst.quemmeviu.com.br/titular/dados-compartilhados/19694?base_legal=1&grouped_ids=19694
Reiniciar para atualizar
Dimensions: iPhone XR 414 x 896 50% No throttling
DevTools is now available in Portug
Don't show again
CANCELAR
Styles
Computed
Layout
POR PTB2
16:03 24/09/2025

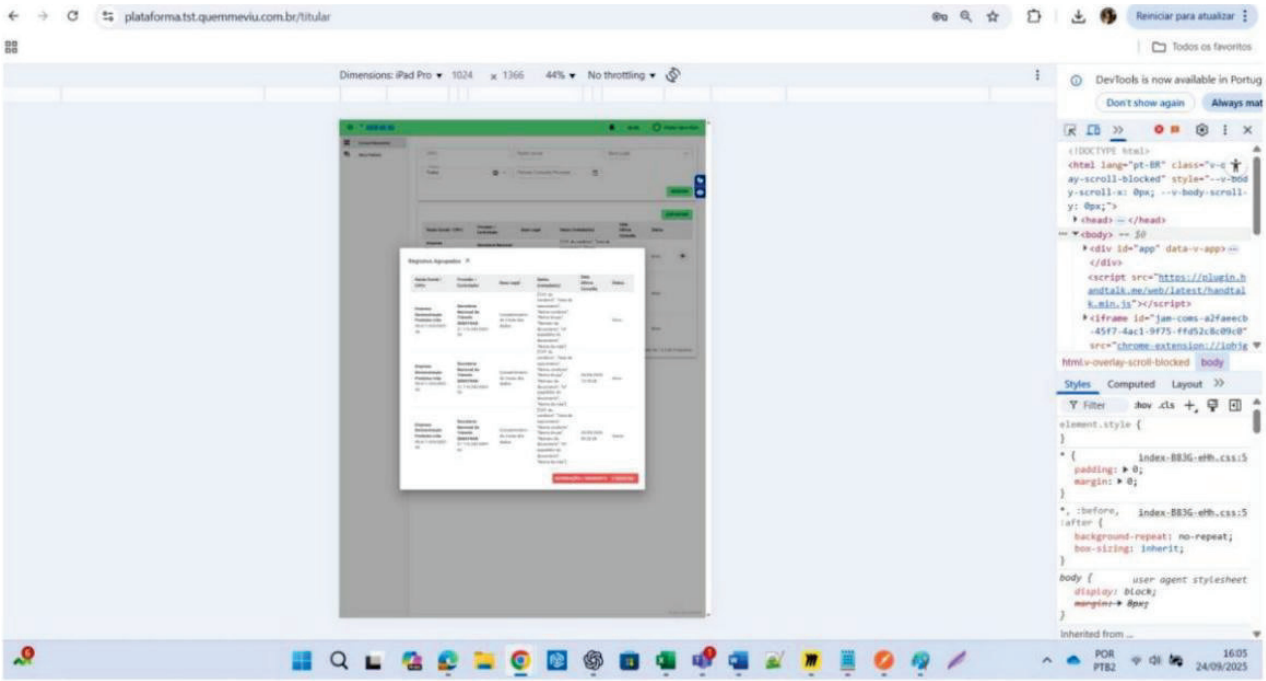

plataforma.tst.quemmeviu.com.br/titular
Reiniciar para atualizar
Dimensions: iPhone XR 414 x 896 50% No throttling
DevTools is now available in Portug
Don't show again
BUSCAR
EXPORTAR
Styles
Computed
Layout
POR PTB2
16:03 24/09/2025

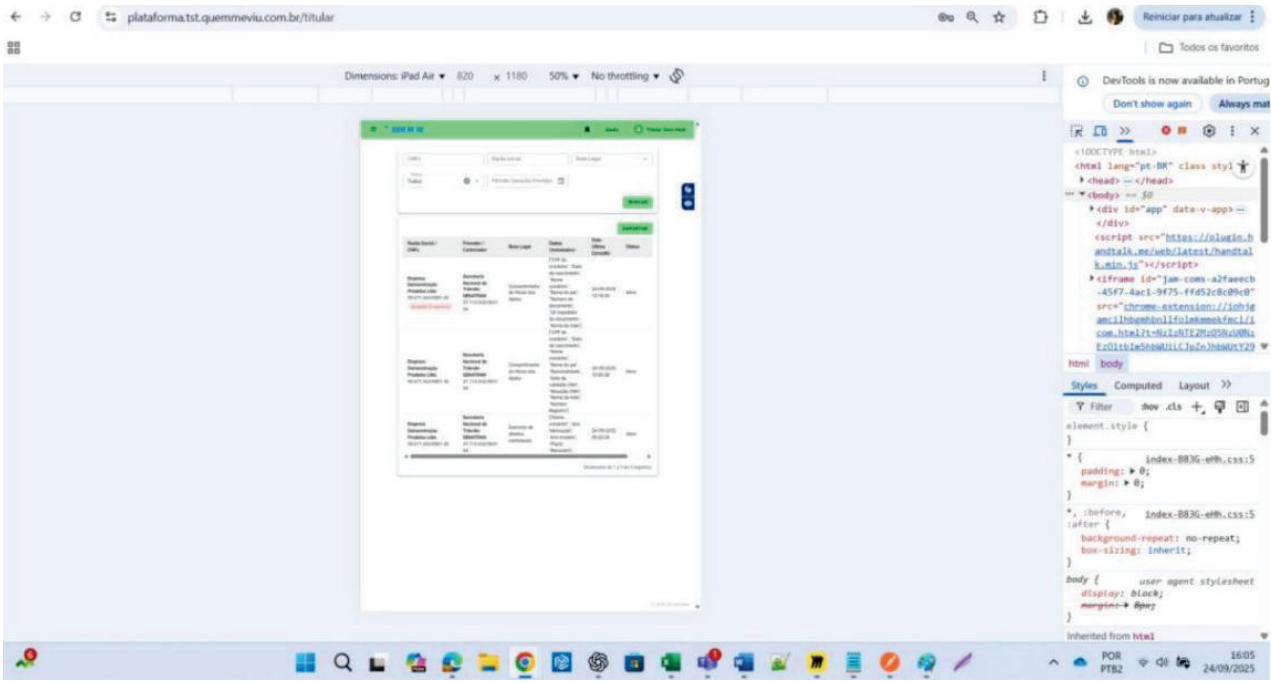

plataforma.tst.quemmeviu.com.br/titular
QUEM ME VIU
CNPJ
Razão social
Base Legal
Status
Todos
Período Consulta Provedor
BUSCAR
EXPORTAR
Razão Social / CNPJ
Provedor / Controlador
Empresa Demonstração Produtos Ltda
99.671.424/0001-45
Secretaria Nacional de Trânsito SENATRAN
37.115.342/0054

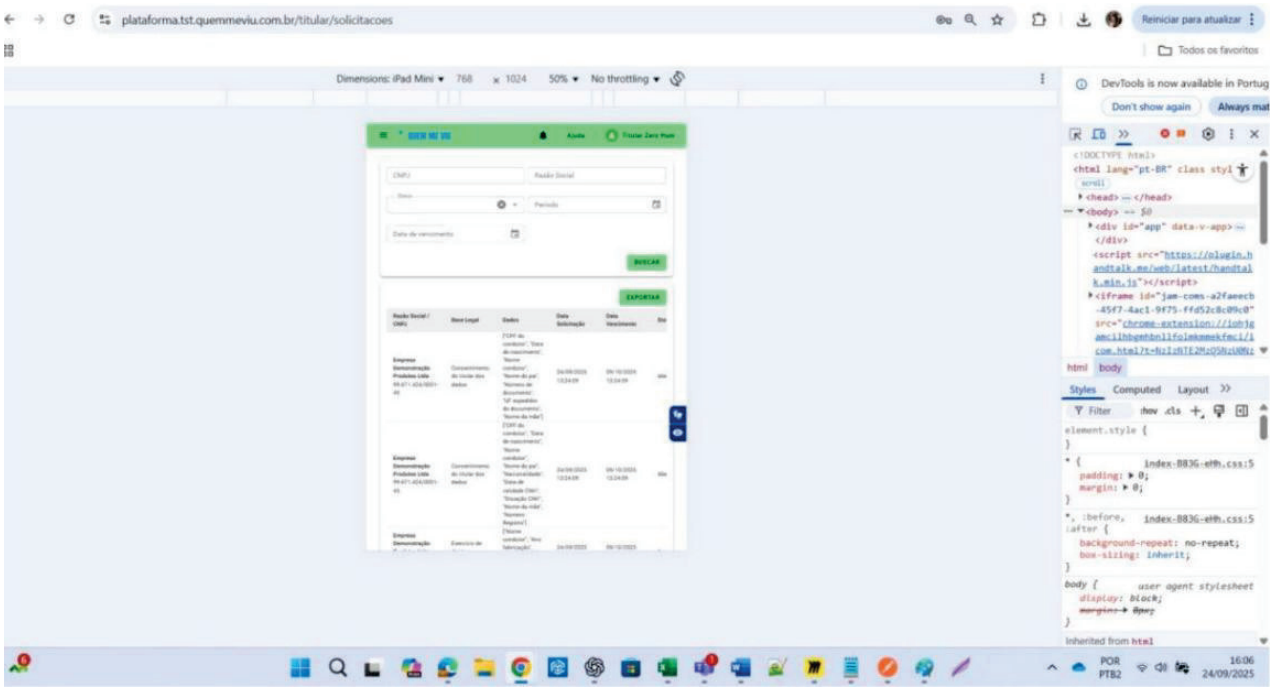

plataforma.tst.quemmeviu.com.br/titular
Razão Social / CNPJ
Provedor / Controlador
Empresa Demonstração Produtos Ltda
99.671.424/0001-45
Secretaria Nacional de Trânsito SENATRAN
37.115.342/0054
Mostrando de 1 a 3 de 3 registros.

Tablet


plataforma.tst.quemmeviu.com.br/titular
Reiniciar para atualizar
Dimensions: iPad Pro 1024 x 1366 44% No throttling
DevTools is now available in Portug
Don't show again
Always mat
Styles
Computed
Layout
element.style {
}
* {
padding: 0;
margin: 0;
}
body {
display: block;
}
POR
PTB2
16:05
24/09/2025


plataforma.tst.quemmeviu.com.br/titular
Reiniciar para atualizar
Dimensions: iPad Pro 1024 x 1366 44% No throttling
DevTools is now available in Portug
Don't show again
Always mat
Styles
Computed
Layout
element.style {
}
* {
padding: 0;
margin: 0;
}
body {
display: block;
}
POR
PTB2
16:05
24/09/2025



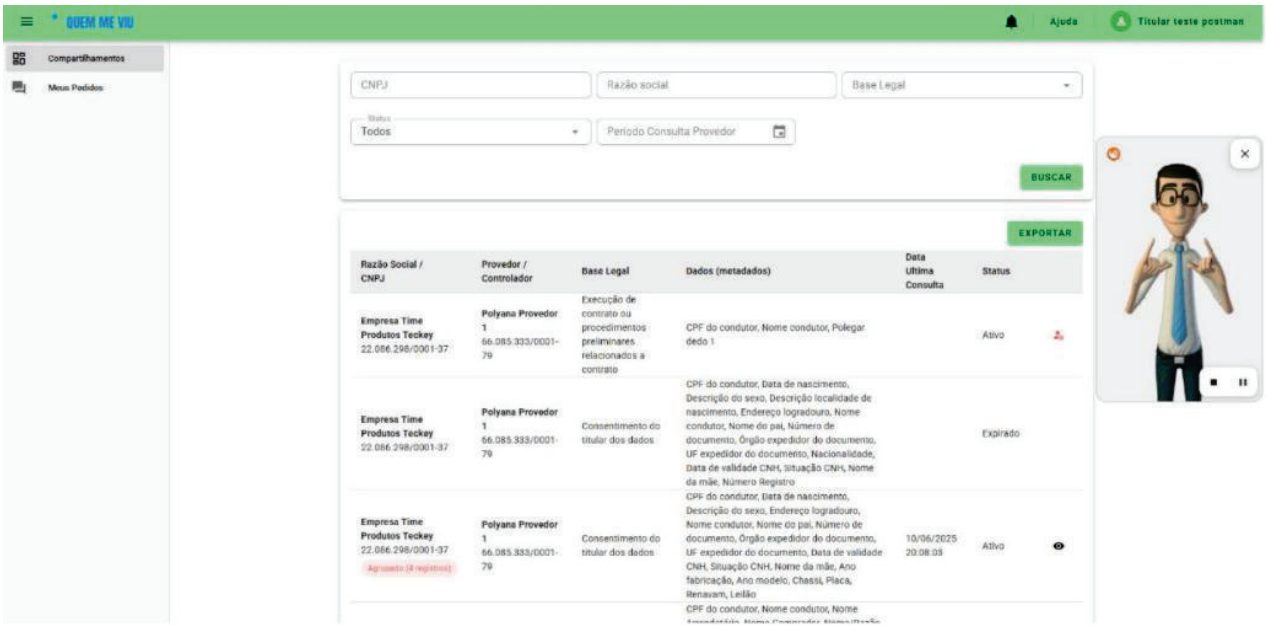


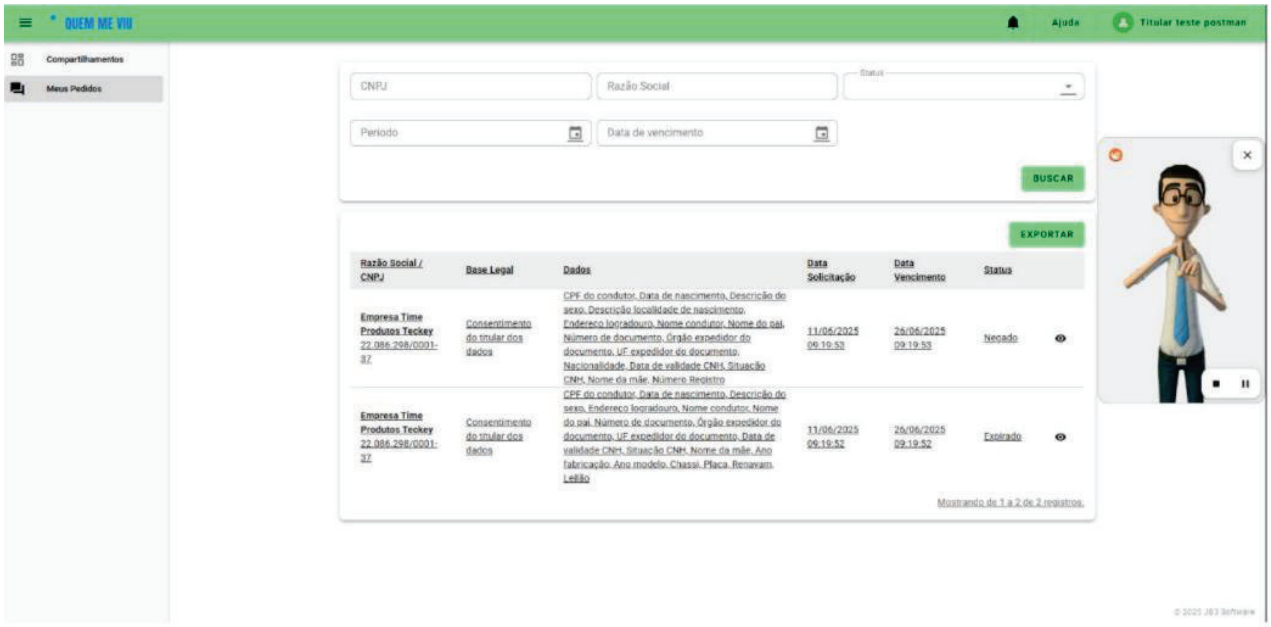
3. Acessibilidade

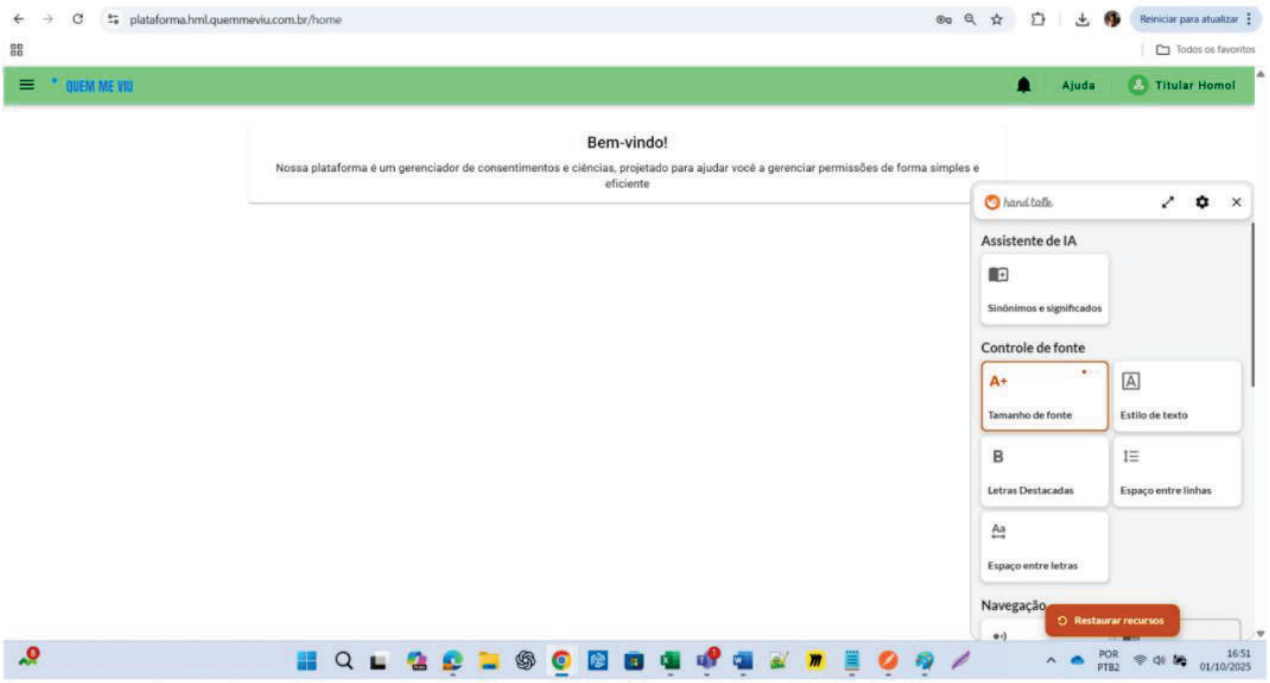
A importância de garantir acessibilidade nas aplicações da GCC está diretamente ligada à inclusão e à conformidade com padrões globais. Aqui estão os principais pontos:

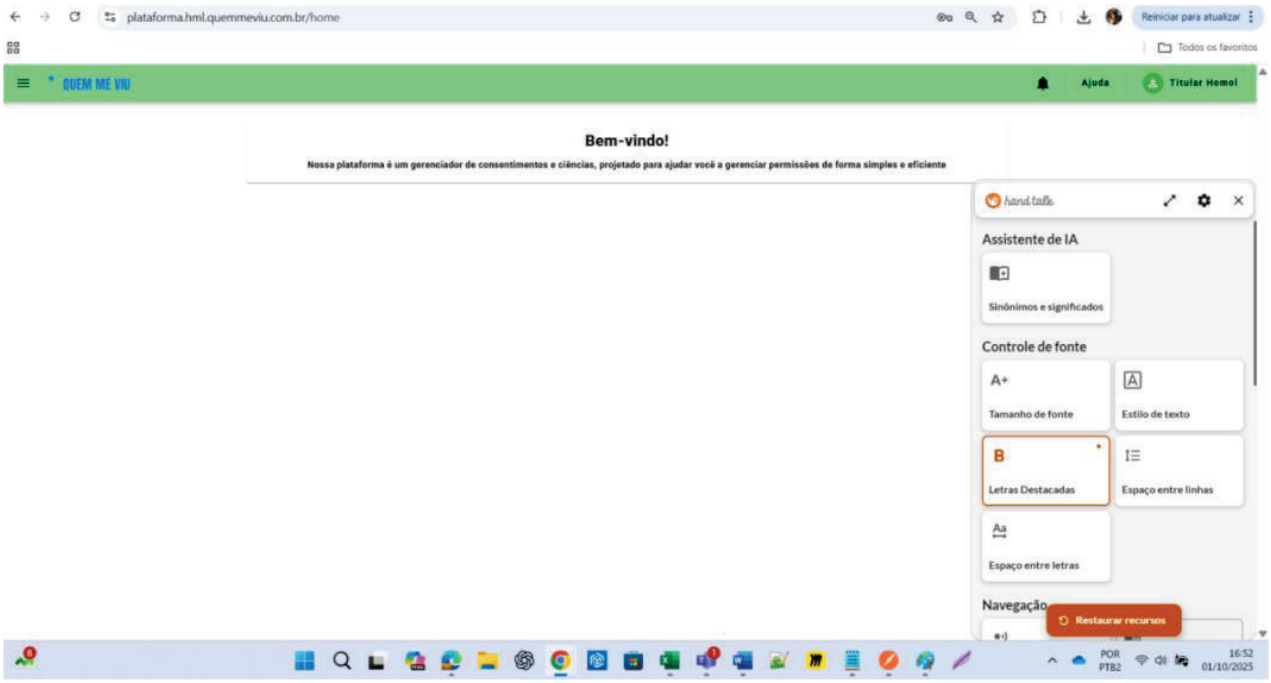
• Inclusão Digital: Permite que pessoas com deficiência visual, auditiva, motora ou cognitiva utilizem as aplicações sem barreiras, garantindo igualdade de acesso à informação e serviços.

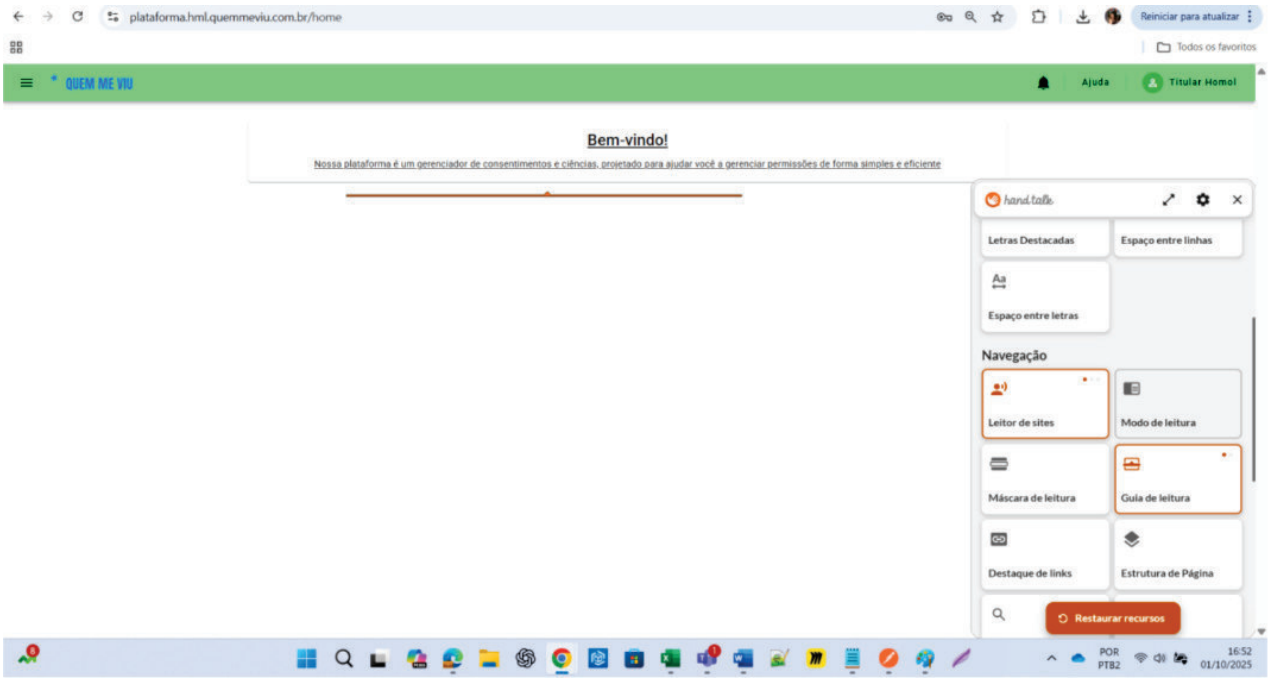
• Conformidade com Normas: Atender às diretrizes da WCAG 2.1 e legislações como a Lei Brasileira de Inclusão (LBI) evita riscos legais e demonstra compromisso com boas práticas.
• Melhoria da Experiência do Usuário: Interfaces acessíveis são mais claras, intuitivas e funcionais para todos os usuários, não apenas para pessoas com deficiência.
• Responsabilidade Social e Reputação: Empresas que priorizam acessibilidade reforçam sua imagem como organizações éticas e comprometidas com diversidade e inclusão.
• Aumento do Alcance: Aplicações acessíveis atingem um público maior, incluindo milhões de pessoas com algum tipo de deficiência, ampliando engajamento e oportunidades de negócio.
Na JB3 utilizamos o plugin da Hand Talk https://www.handtalk.me/br/ , o mais inovador ecossistema de acessibilidade digital. A pessoa usuária poderá acessar o tradutor de sites (língua de sinais) e utilizar uma série de recursos assistidos como controle de fonte, estilo de texto, letras destacadas, espaços entre linhas, espaço entre letras, leitor de sites, modo de leitura, máscara de leitura, guia de leitura, destaque de links, estrutura de página, lupa de conteúdo, esconder imagens, destacar cabeçalho, pausar animações, parar sons, controle de cor, entre outros.

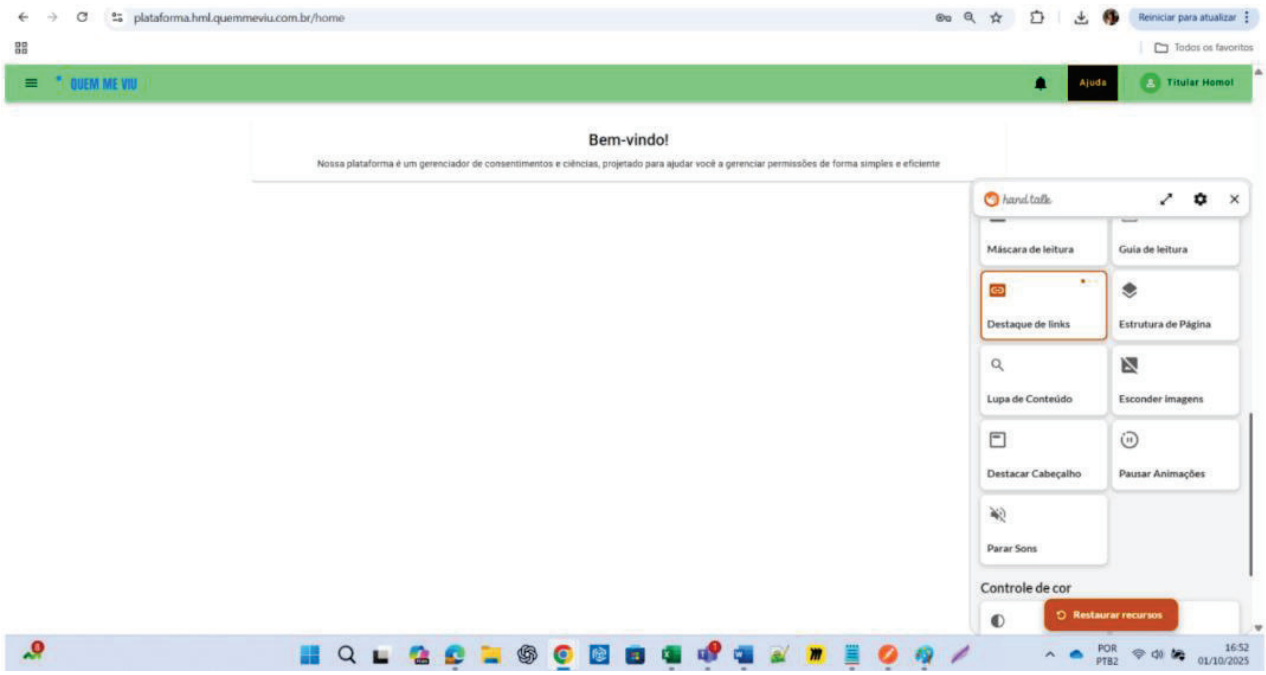

QUEM ME VIU
Ajuda
Titular teste postman
Compartilhamentos
Meus Pedidos
CNPJ
Razão social
Base Legal
Status
Todos
Período Consulta Provedor
BUSCAR
EXPORTAR
Razão Social / CNPJ
Provedor / Controlador
Base Legal
Dados (metadados)
Data Ultima Consulta
Status
Empresa Time Produtos Teckey 22.086.298/0001-37
Polyana Provedor 1 66.085.333/0001-79
Execução de contrato ou procedimentos preliminares relacionados a contrato
CPF do condutor, Nome condutor, Polegar dedo 1
Ativo
Consentimento do titular dos dados
CPF do condutor, Data de nascimento, Descrição do sexo, Descrição localidade de nascimento, Endereço logradouro, Nome condutor, Nome do pai, Número de documento, Órgão expedidor do documento, UF expedidor do documento, Nacionalidade, Data de validade CNH, Situação CNH, Nome da mãe, Número Registro
Expirado
CPF do condutor, Data de nascimento, Descrição do sexo, Endereço logradouro, Nome condutor, Nome do pai, Número de documento, Órgão expedidor do documento, UF expedidor do documento, Data de validade CNH, Situação CNH, Nome da mãe, Ano fabricação, Ano modelo, Chassi, Placa, Renavam, Leilão
10/06/2025 20:08:08
Ativo

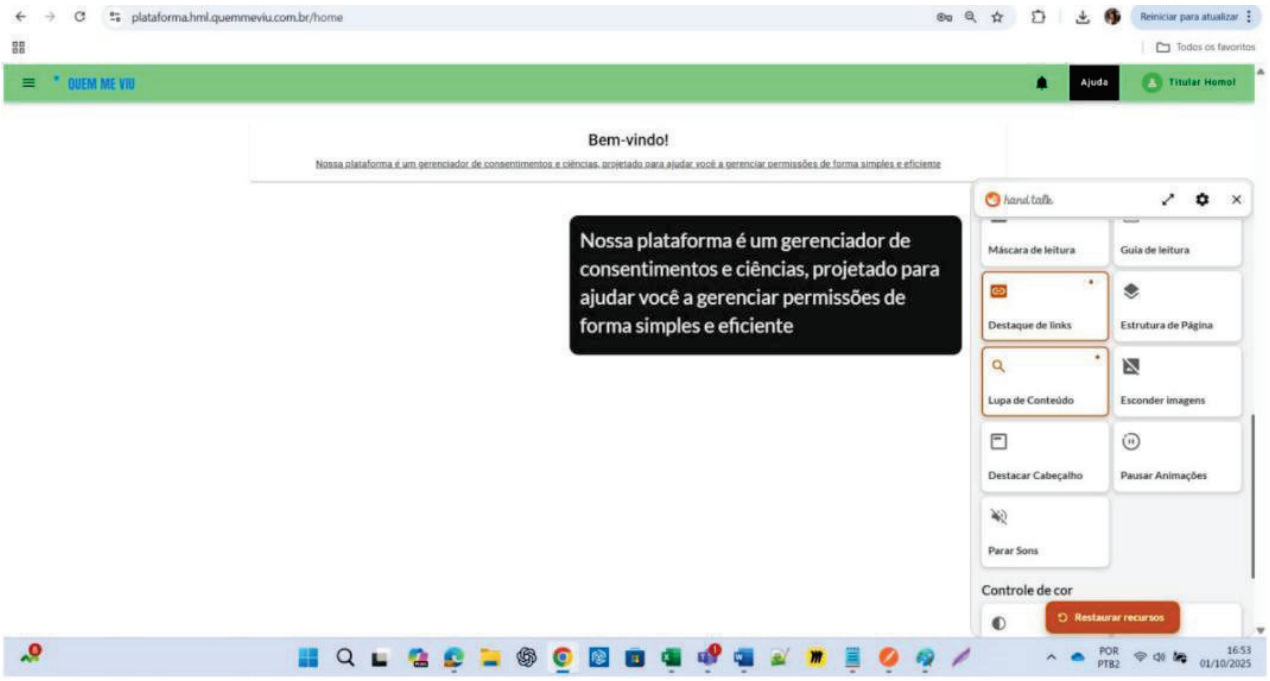

QUEM ME VIU
Ajuda
Titular teste postman
Compartilhamentos
Meus Pedidos
CNPJ
Razão Social
Status
Período
Data de vencimento
BUSCAR
EXPORTAR
Razão Social / CNPJ
Base Legal
Dados
Data Solicitação
Data Vencimento
Status
Empresa Time Produtos Teckey 22.086.298/0001-37
Consentimento do titular dos dados
CPF do condutor, Data de nascimento, Descrição do sexo, Descrição localidade de nascimento, Endereço logradouro, Nome condutor, Nome do pai, Número de documento, Órgão expedidor do documento, UF expedidor do documento, Nacionalidade, Data de validade CNH, Situação CNH, Nome da mãe, Número Registro
11/06/2025 09:19:53
26/06/2025 09:19:53
Negado
CPF do condutor, Data de nascimento, Descrição do sexo, Endereço logradouro, Nome condutor, Nome do pai, Número de documento, Órgão expedidor do documento, UF expedidor do documento, Data de validade CNH, Situação CNH, Nome da mãe, Ano fabricação, Ano modelo, Chassi, Placa, Renavam, Leilão
11/06/2025 09:19:52
26/06/2025 09:19:52
Expirado
Mostrando de 1 a 2 de 2 registros.

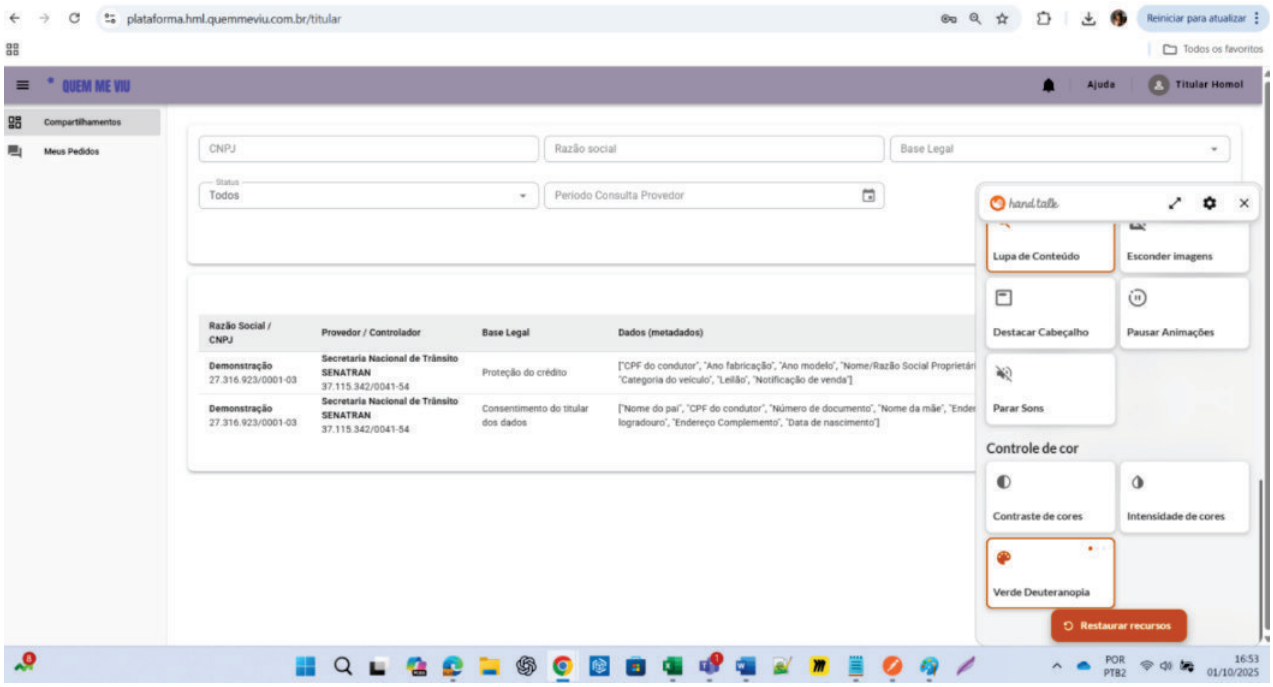

plataforma.hml.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Homol
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Assistente de IA
Sinônimos e significados
Controle de fonte
Tamanho de fonte
Estilo de texto
Letras Destacadas
Espaço entre linhas
Espaço entre letras
Navegação
Restaurar recursos


plataforma.hml.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Homol
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Assistente de IA
Sinônimos e significados
Controle de fonte
Tamanho de fonte
Estilo de texto
Letras Destacadas
Espaço entre linhas
Espaço entre letras
Navegação
Restaurar recursos


plataforma.hml.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Homol
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Letras Destacadas
Espaço entre linhas
Espaço entre letras
Navegação
Leitor de sites
Modo de leitura
Máscara de leitura
Guia de leitura
Destaque de links
Estrutura de Página
Restaurar recursos


plataforma.hml.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Homol
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Máscara de leitura
Guia de leitura
Destaque de links
Estrutura de Página
Lupa de Conteúdo
Esconder Imagens
Destacar Cabeçalho
Pausar Animações
Parar Sons
Controle de cor
Restaurar recursos


plataforma.hml.quemmeviu.com.br/home
QUEM ME VIU
Ajuda
Titular Homol
Bem-vindo!
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
Nossa plataforma é um gerenciador de consentimentos e ciências, projetado para ajudar você a gerenciar permissões de forma simples e eficiente
hand talk
Máscara de leitura
Guia de leitura
Destaque de links
Estrutura de Página
Lupa de Conteúdo
Esconder imagens
Destacar Cabeçalho
Pausar Animações
Parar Sons
Controle de cor
Restaurar recursos


plataforma.hml.quemmeviu.com.br/titular
QUEM ME VIU
Ajuda
Titular Homol
Compartilhamentos
Meus Pedidos
CNPJ
Razão social
Base Legal
Status
Todos
Período Consulta Provedor
Razão Social / CNPJ
Provedor / Controlador
Base Legal
Dados (metadados)
Demonstração 27.316.923/0001-03
Secretaria Nacional de Trânsito SENATRAN 37.115.342/0041-54
Proteção do crédito
Demonstração 27.316.923/0001-03
Secretaria Nacional de Trânsito SENATRAN 37.115.342/0041-54
Consentimento do titular dos dados
hand talk
Lupa de Conteúdo
Esconder imagens
Destacar Cabeçalho
Pausar Animações
Parar Sons
Controle de cor
Contraste de cores
Intensidade de cores
Verde Deuteranopia
Restaurar recursos

4. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

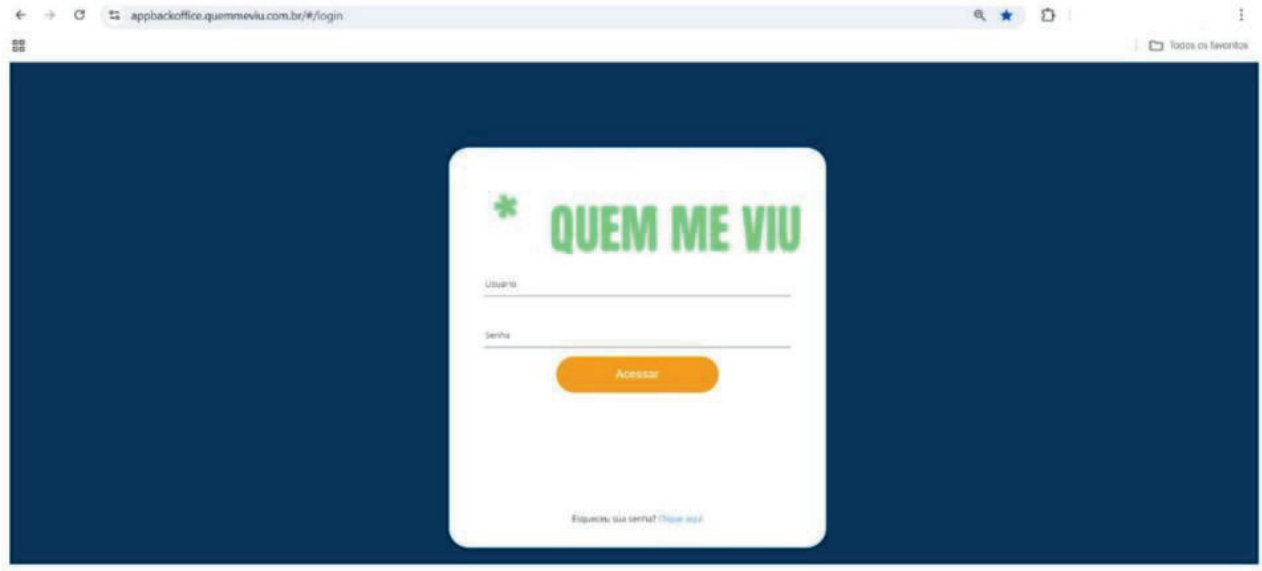
1. Objetivo

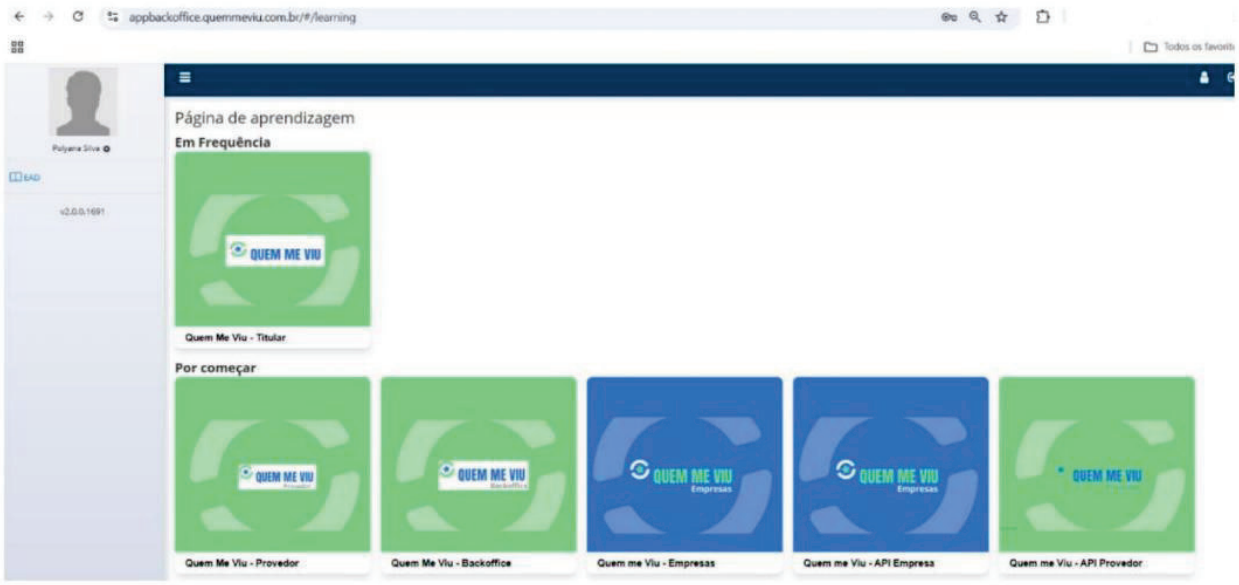
Garantir que a GCC possua capacidade de disponibilizar treinamentos técnicos e operacionais à distância (EAD), com:
Instrutores certificados e experientes, assegurando qualidade e credibilidade do conteúdo.
Plataforma digital acessível e responsiva, permitindo aprendizado remoto com flexibilidade.
Conteúdo atualizado e alinhado às melhores práticas, cobrindo aspectos técnicos, operacionais e regulatórios.
Recursos interativos e suporte ao aluno, para promover engajamento e eficácia no aprendizado.
Essa capacidade contribui para padronização de processos, qualificação contínua e conformidade com requisitos legais e técnicos.

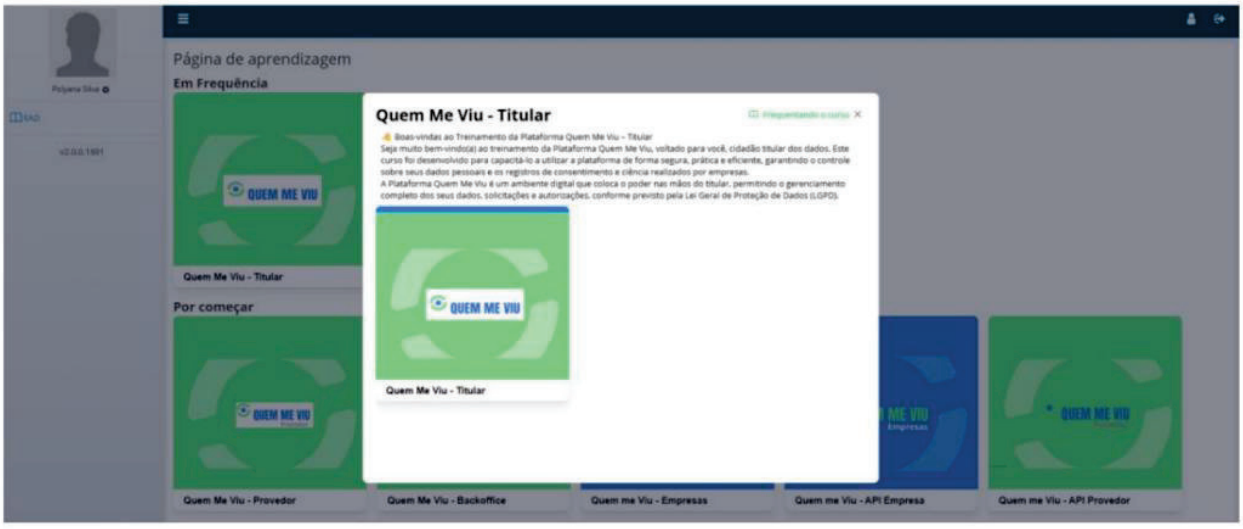
2. Plataforma EAD

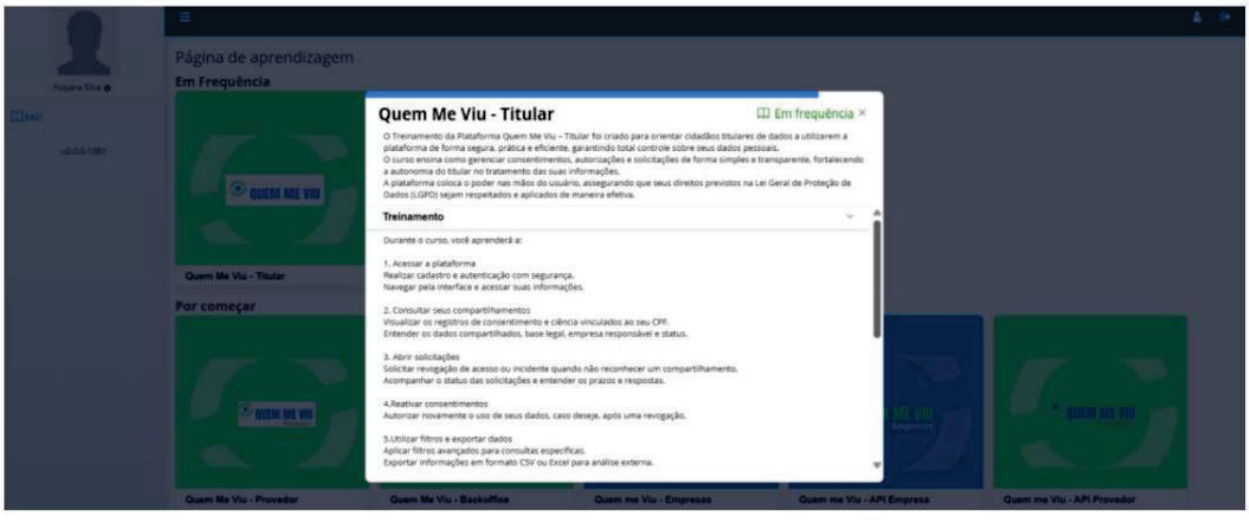
A plataforma de Ensino à Distância (EAD) da GCC foi desenvolvida para capacitar usuários de forma prática e acessível, oferecendo:
• Módulos de treinamento organizados por plataforma e por API, garantindo aprendizado segmentado e direcionado.
• Cursos completos, com conteúdos técnicos e operacionais atualizados.
• Quiz interativo de perguntas e respostas, para reforçar conhecimento e avaliar desempenho.
• Emissão automática de certificado ao término do curso, validando a conclusão e a qualificação do participante.
Essa estrutura promove flexibilidade, engajamento e padronização do conhecimento, assegurando que todos os usuários estejam preparados para operar e integrar soluções da GCC.

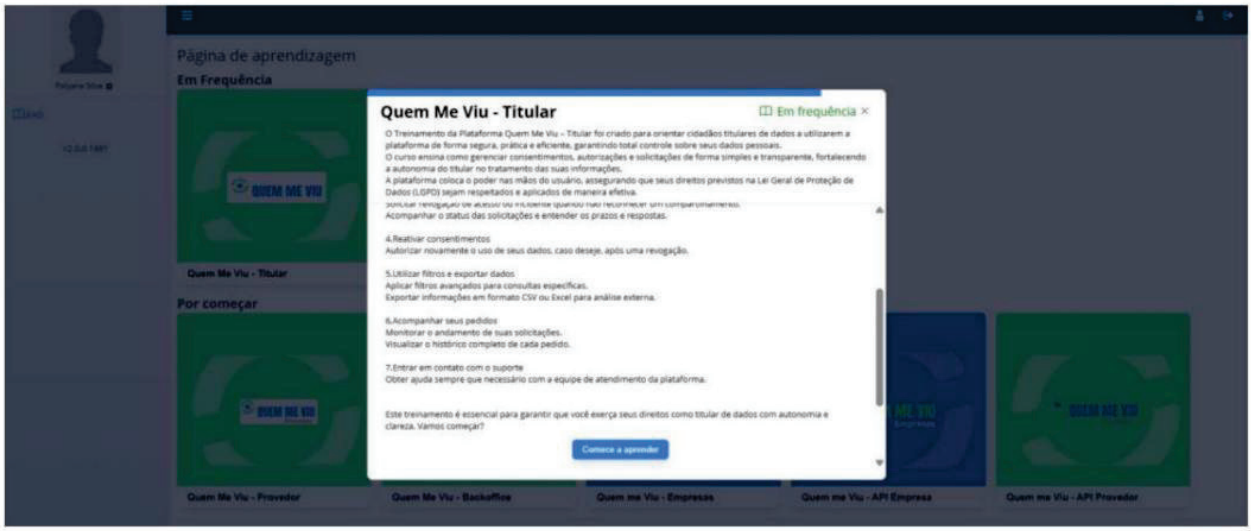
https://appbackoffice.quemmeviu.com.br/#/login

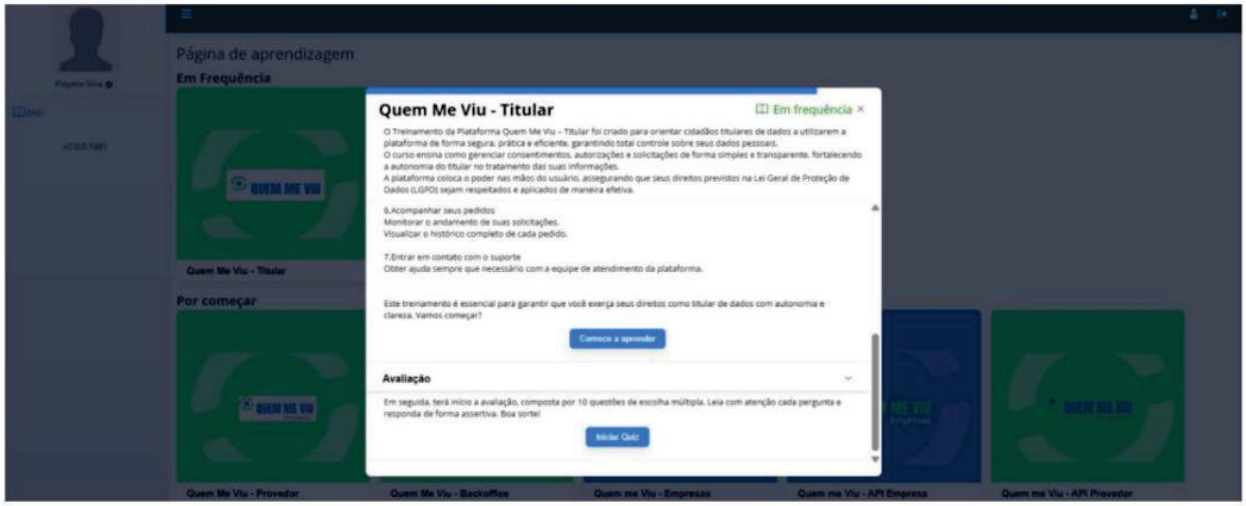



appbackoffice.quemmeviu.com.br/#/learning
Página de aprendizagem
Em Frequência
Quem Me Viu - Titular
Por começar
Quem Me Viu - Provedor
Quem Me Viu - Backoffice
Quem me Viu - Empresas
Quem me Viu - API Empresa
Quem me Viu - API Provedor


Página de aprendizagem
Em Frequência
Quem Me Viu - Titular
Boas-vindas ao Treinamento da Plataforma Quem Me Viu - Titular
Seja muito bem-vindo(a) ao treinamento da Plataforma Quem Me Viu, voltado para você, cidadão titular dos dados. Este curso foi desenvolvido para capacitá-lo a utilizar a plataforma de forma segura, prática e eficiente, garantindo o controle sobre seus dados pessoais e os registros de consentimento e ciência realizados por empresas.
A Plataforma Quem Me Viu é um ambiente digital que coloca o poder nas mãos do titular, permitindo o gerenciamento completo dos seus dados, solicitações e autorizações, conforme previsto pela Lei Geral de Proteção de Dados (LGPD).
Por começar
Quem Me Viu - Provedor
Quem Me Viu - Backoffice
Quem me Viu - Empresas
Quem me Viu - API Empresa
Quem me Viu - API Provedor


Página de aprendizagem
Em Frequência
Quem Me Viu - Titular
Em frequência
O Treinamento da Plataforma Quem Me Viu – Titular foi criado para orientar cidadãos titulares de dados a utilizarem a plataforma de forma segura, prática e eficiente, garantindo total controle sobre seus dados pessoais.
O curso ensina como gerenciar consentimentos, autorizações e solicitações de forma simples e transparente, fortalecendo a autonomia do titular no tratamento das suas informações.
A plataforma coloca o poder nas mãos do usuário, assegurando que seus direitos previstos na Lei Geral de Proteção de Dados (LGPD) sejam respeitados e aplicados de maneira efetiva.
Treinamento
Durante o curso, você aprenderá a:
1. Acessar a plataforma
Realizar cadastro e autenticação com segurança.
Navegar pela interface e acessar suas informações.
2. Consultar seus compartilhamentos
Visualizar os registros de consentimento e ciência vinculados ao seu CPF.
Entender os dados compartilhados, base legal, empresa responsável e status.
3. Abrir solicitações
Solicitar revogação de acesso ou incidente quando não reconhecer um compartilhamento.
Acompanhar o status das solicitações e entender os prazos e respostas.
4.Reativar consentimentos
Autorizar novamente o uso de seus dados, caso deseje, após uma revogação.
5.Utilizar filtros e exportar dados
Aplicar filtros avançados para consultas específicas.
Exportar informações em formato CSV ou Excel para análise externa.
Por começar
Quem Me Viu - Provedor
Quem Me Viu - Backoffice
Quem me Viu - Empresas
Quem me Viu - API Empresa
Quem me Viu - API Provedor


Página de aprendizagem
Em Frequência
Quem Me Viu - Titular
Em frequência
O Treinamento da Plataforma Quem Me Viu - Titular foi criado para orientar cidadãos titulares de dados a utilizarem a plataforma de forma segura, prática e eficiente, garantindo total controle sobre seus dados pessoais.
O curso ensina como gerenciar consentimentos, autorizações e solicitações de forma simples e transparente, fortalecendo a autonomia do titular no tratamento das suas informações.
A plataforma coloca o poder nas mãos do usuário, assegurando que seus direitos previstos na Lei Geral de Proteção de Dados (LGPD) sejam respeitados e aplicados de maneira efetiva.
Acompanhar o status das solicitações e entender os prazos e respostas.
4.Reativar consentimentos
Autorizar novamente o uso de seus dados, caso deseje, após uma revogação.
5.Utilizar filtros e exportar dados
Aplicar filtros avançados para consultas específicas.
Exportar informações em formato CSV ou Excel para análise externa.
6.Acompanhar seus pedidos
Monitorar o andamento de suas solicitações.
Visualizar o histórico completo de cada pedido.
7.Entrar em contato com o suporte
Obter ajuda sempre que necessário com a equipe de atendimento da plataforma.
Este treinamento é essencial para garantir que você exerça seus direitos como titular de dados com autonomia e clareza. Vamos começar?
Começa a aprender
Por começar
Quem Me Viu - Titular
Quem Me Viu - Provedor
Quem Me Viu - Backoffice
Quem me Viu - Empresas
Quem me Viu - API Empresa
Quem me Viu - API Provedor


Página de aprendizagem
Em Frequência
Quem Me Viu - Titular
Em frequência
O Treinamento da Plataforma Quem Me Viu - Titular foi criado para orientar cidadãos titulares de dados a utilizarem a plataforma de forma segura, prática e eficiente, garantindo total controle sobre seus dados pessoais.
O curso ensina como gerenciar consentimentos, autorizações e solicitações de forma simples e transparente, fortalecendo a autonomia do titular no tratamento das suas informações.
A plataforma coloca o poder nas mãos do usuário, assegurando que seus direitos previstos na Lei Geral de Proteção de Dados (LGPD) sejam respeitados e aplicados de maneira efetiva.
6.Acompanhar seus pedidos
Monitorar o andamento de suas solicitações.
Visualizar o histórico completo de cada pedido.
7.Entrar em contato com o suporte
Obter ajuda sempre que necessário com a equipe de atendimento da plataforma.
Este treinamento é essencial para garantir que você exerça seus direitos como titular de dados com autonomia e clareza. Vamos começar?
Começa a aprender
Avaliação
Em seguida, terá início a avaliação, composta por 10 questões de escolha múltipla. Leia com atenção cada pergunta e responda de forma assertiva. Boa sorte!
Iniciar Quiz
Por começar
Quem Me Viu - Titular
Quem Me Viu - Provedor
Quem Me Viu - Backoffice
Quem me Viu - Empresas
Quem me Viu - API Empresa
Quem me Viu - API Provedor


appbackoffice.quemmeviu.com.br/#/learning
Novo Chrome disponível
Página de aprendizagem
Cursos concluídos com sucesso
Quem Me Viu - Titular
Quem Me Viu - Provedor
Quem Me Viu - Backoffice
Quem me Viu - Empresas
Quem me Viu - API Empresa
Quem me Viu - API Provedor

QUEM ME VIU

Certificado de Conclusão de Curso

Certificamos que, após participação e cumprimento dos requisitos, o participante concluiu com sucesso o curso descrito abaixo.

Nome do Participante:

Polyana Silva

Curso:

Quem Me Viu - Provedor

Data de conclusão: **2025-10-20**

Certificamos que o(a) **Polyana Silva** participou ativamente e concluiu com sucesso o curso **Quem Me Viu - Provedor**, cumprindo as atividades e avaliações previstas no programa.

Este certificado é válido como comprovação de participação e conclusão do curso para fins de registro e comprovação acadêmica /profissional, conforme as políticas internas da instituição.

3. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

POLÍTICA DE GESTÃO DE CRISES, RESPOSTAS A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PLANO DE CONTINUIDADE DAS OPERAÇÕES

1. Introdução

Esta política estabelece os princípios, conceitos, diretrizes e responsabilidades para a gestão de Crises e Respostas a Incidentes de Segurança da Informação na JB3 SOFTWARES S.A., abrangendo tanto incidentes cibernéticos quanto físicos. Incluem incidentes que envolvem dados pessoais e dados pessoais sensíveis, sistemas digitais e ativos físicos que possam impactar os negócios. O propósito é assegurar que todos os incidentes sejam tratados adequadamente, minimizando impactos nos negócios, garantindo a integridade dos sistemas, proteção de dados pessoais e segurança física, preservando a confiabilidade das marcas e serviços desta empresa, bem como, ações para continuidade das operações, garantindo a proteção dos dados e ativos de informação visando a manutenção da prestação de serviços essenciais, em conformidade com a legislação vigente, especialmente a **Lei nº 13.709/2018 (LGPD)** e **Decreto nº 10.222/2020 (E-Ciber.), bem como, a ISO 27001 (Segurança da Informação) e ISO 22301 (Continuidade de Negócios).**

2. Abrangência

Esta política tem abrangência corporativa e se aplica a todos os casos de Crises e Incidentes de Segurança da Informação, sejam cibernéticos ou físicos. Deve ser cumprida por todas as áreas de negócio e colaboradores, incluindo sócios, diretores, administradores, empregados, prestadores de serviços e parceiros que possuam acesso a áreas, equipamentos, informações, redes e dados da JB3 SOFTWARES S.A.

3. Diretrizes

Todos os colaboradores devem estar preparados para identificar e notificar eventos e incidentes de segurança da informação e privacidade ou fragilidades observadas que possam causar:

Prejuízos;

Interrupções;

Maus funcionamentos;

Imprecisão;

Vazamento de dados nos sistemas e ambientes.

Todos os eventos de incidente de segurança da informação e privacidade devem ser registrados nos controles e/ou ferramentas para a devida triagem e tratamento;

Os eventos de incidente de segurança da informação e privacidade devem ser categorizados e classificados através de uma matriz de severidade com intuito de se ter uma melhor visibilidade, tratamento e prioridade quanto a sua gestão;

O conteúdo da notificação precisa ser claro, em formato simples e deve incluir as informações necessárias para a rápida e correta identificação do problema e da ação requerida;

Violações ou tentativas de violação da Diretriz de Segurança da Informação, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

Incidentes de segurança podem ser identificados por processos de monitoramento da área de infraestrutura por Colaboradores que observem fragilidades, anomalias e violações que coloquem a segurança da empresa em risco.

Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos colaboradores, sob o risco de violar a política de segurança da informação, bem como provocar danos aos serviços ou recursos tecnológicos.

É de extrema importância que o horário de servidores e equipamentos de redes estejam sincronizados com uma fonte confiável de tempo (ex: via protocolo NTP) para que não haja disparidades na correlação de eventos, logs e outros dados.

Deve ser comunicado os incidentes de segurança da informação e privacidade de acordo com a severidade do incidente

4. Incidente de Segurança e Privacidade

São considerados Incidentes de Segurança da Informação e Privacidade quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade, incluindo segurança física e proteção de ativos e colocando o negócio e seus objetivos em risco ou à imagem desta empresa.

Abaixo relacionamos alguns possíveis incidentes de segurança e privacidade, não se limitando:

Violações de políticas de segurança ou controles estabelecidos;

Perda ou corrupção de dados por desastres naturais;

Indisponibilidade por ataques maliciosos;

Vazamento ou roubo de informações;

Tentativas de acesso não autorizado;

Uso ou acesso indevido a dados ou sistemas;

Modificações não autorizadas em sistemas;

Tratamento incorreto de dados pessoais fora da finalidade declarada;

Descarte incorreto de documentos sigilosos, bem como compartilhamento inadequado de senhas pessoais;

Violação de acesso físico a áreas críticas;

Danos físicos intencionais a ativos da organização;

E, incidentes, falhas de infraestrutura ou ataques cibernéticos.

5. Definições

Segurança da Informação: Proteção da confidencialidade, integridade e disponibilidade das informações.

Incidente de Segurança da Informação: Evento que comprometa ou possa comprometer dados, sistemas ou serviços, bem como, a confidencialidade, integridade ou disponibilidade das informações.

Crise: Situação grave que afeta de forma significativa a operação, imagem ou a segurança de dados e requer ação coordenada imediata.

Plano de Continuidade das Operações (PCO): Estratégia e conjunto de procedimentos para garantir a manutenção ou rápida retomada das atividades críticas da organização após incidentes ou interrupções.

TRI – Time de Resposta a Incidentes: Equipe designada para investigar, mitigar, erradicar e registrar incidentes de segurança.

6. Princípios Gerais

Prevenção: Por meio de controles técnicos e administrativos visando implementar controles para reduzir a probabilidade de incidentes.

Detecção: Identificar de forma tempestiva qualquer evento anormal.

Resposta ágil: Atuar de maneira coordenada para conter danos e restaurar serviços.

Comunicação transparente: Informar as partes interessadas e autoridades competentes conforme exigido por lei.

Aprendizado contínuo: Incorporar lições aprendidas para aprimorar processos e controles.

7. Política de Segurança da Informação para Gestão de Crises

Durante a gestão de crises, especialmente as relacionadas à segurança da informação, a JB3 SOFTWARES S.A. adota os seguintes princípios e diretrizes adicionais:

Proteção da Informação

● Restringir o acesso a dados e sistemas críticos apenas a pessoal autorizado.

● Utilizar mecanismos de autenticação forte e segregação de funções.

● Implementar controles adicionais de monitoramento para detectar atividades anômalas.

Continuidade da Confidencialidade, Integridade e Disponibilidade

● Garantir que dados e serviços críticos sejam preservados durante a crise, com backups atualizados e redundâncias ativas.

● Utilizar canais seguros para comunicação interna e externa durante a crise.

● Proibir o uso de dispositivos ou redes não autorizados.

Gestão de Comunicação Segura

● Centralizar a comunicação oficial no Comitê de Crise.

● Garantir que todas as informações divulgadas sejam verificadas e autorizadas.

● Utilizar criptografia e ferramentas seguras para compartilhamento de dados.

Proteção contra Ameaças Internas e Externas

● Monitorar atividades suspeitas de usuários internos.

● Bloquear tentativas de acesso não autorizado.

● Reforçar controles contra ataques cibernéticos (DDoS, ransomware, phishing).

Registro e Auditoria:

● Registrar todas as ações tomadas durante a crise para posterior auditoria.

● Manter relatórios detalhados para análise pós-incidente.

8. Estrutura e Responsabilidades

Colaboradores: Reportar imediatamente incidentes ou suspeitas.

TRI – Time de Resposta a Incidentes: Avaliar, conter e erradicar incidentes, além de apoiar a recuperação.

Gestores: Disponibilizar recursos, apoiar a execução desta política e ações emergenciais.

DPO/Encarregado LGPD: Coordenar ações em casos envolvendo dados pessoais.

Comitê de Crise: Integrar representantes da alta direção, TI, jurídico e comunicação, responsável por decisões estratégicas em eventos de grande impacto.

9. Procedimentos de Resposta a Incidentes

Identificação do incidente.

Notificação ao canal oficial.

Classificação e determinação da gravidade (baixo, médio, alto, crítico).

Contenção com ações imediatas para impedir agravamento do impacto.

Erradicação e eliminação da causa raiz.

Recuperação e restauração segura dos serviços afetados.

Pós-incidente elaborar relatório de análise de impacto e medidas preventivas.

10. Comunicação de Incidentes

CANAL OFICIAL: seguranca@jb3ti.com.br.

Notificação às autoridades competentes, incluindo ANPD, TCU, CGU, MPF ou outros órgãos, no prazo legal ou contratual.

Comunicação aos titulares de dados, quando aplicável.

11. Gestão de Crises

O Comitê de Crise será acionado em eventos de alto impacto.

As ações incluem:

- Avaliação de riscos.
- Definição de estratégias emergenciais.
- Coordenação de comunicação com clientes, órgãos reguladores e imprensa.
- Priorização da continuidade dos serviços essenciais.

12. Plano de Continuidade das Operações (pco)

O PCO tem como finalidade assegurar que, em caso de interrupções, as operações críticas da JB3 SOFTWARES S.A. sejam mantidas ou retomadas no menor tempo possível.

Identificação de processos críticos: Listagem dos serviços e sistemas essenciais para o negócio.

Análise de Impacto nos Negócios (BIA): Avaliação dos efeitos de interrupções prolongadas.

Definição de RTO/RPO:

- RTO (Recovery Time Objective) – tempo máximo para restabelecer o serviço.
- RPO (Recovery Point Objective) – perda máxima aceitável de dados.

Recursos de contingência:

- Backup diário de dados.
- Redundância de servidores e links de internet.
- Serviços em nuvem para mitigação de falhas físicas.

Procedimentos de recuperação: Passo a passo para retorno seguro das operações.

Testes periódicos: Simulações semestrais para validar o PCO.

Plano de comunicação de crise: Roteiro para informar clientes, parceiros e órgãos reguladores sobre a situação e medidas adotadas.

13. Treinamento e Conscientização

Treinamentos anuais obrigatórios sobre segurança da informação e gestão de crises para os colaboradores.

Simulações práticas de incidentes e crises para aprimorar as respostas e o PCO.

14. Revisão e Atualização

Esta política será revisada anualmente ou após incidentes relevantes. Alterações devem ser aprovadas pela alta direção da JB3 SOFTWARES S.A.

15. Vigência

Esta política entra em vigor na data de sua aprovação e revoga quaisquer versões anteriores.

16. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
POLÍTICA DE GESTÃO DE CRISES, RESPOSTAS A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PLANO DE CONTINUIDADE DAS OPERAÇÕES	Manual de Procedimentos	30/04/2025	1.0

Data	Descrição Ação	Versão	Responsável
30/04/2025	Elaboração	1.0	Jurídico
30/04/2025	Revisado e Aprovado	2.0	Diretoria Executiva

POLÍTICA DE GESTÃO DE CRISES, RESPOSTAS A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PLANO DE CONTINUIDADE DAS OPERAÇÕES

1. Introdução

Esta política estabelece os princípios, conceitos, diretrizes e responsabilidades para a gestão de Crises e Respostas a Incidentes de Segurança da Informação na JB3 SOFTWARES S.A., abrangendo tanto incidentes cibernéticos quanto físicos. Incluem incidentes que envolvem dados pessoais e dados pessoais sensíveis, sistemas digitais e ativos físicos que possam impactar os negócios. O propósito é assegurar que todos os incidentes sejam tratados adequadamente, minimizando impactos nos negócios, garantindo a integridade dos sistemas, proteção de dados pessoais e segurança física, preservando a confiabilidade das marcas e serviços desta empresa, bem como, ações para continuidade das operações, garantindo a proteção dos dados e ativos de informação visando a manutenção da prestação de serviços essenciais, em conformidade com a legislação vigente, especialmente a **Lei nº 13.709/2018 (LGPD)** e **Decreto nº 10.222/2020 (E-Ciber.), bem como, a ISO 27001 (Segurança da Informação) e ISO 22301 (Continuidade de Negócios).**

2. Abrangência

Esta política tem abrangência corporativa e se aplica a todos os casos de Crises e Incidentes de Segurança da Informação, sejam cibernéticos ou físicos. Deve ser cumprida por todas as áreas de negócio e colaboradores, incluindo sócios, diretores, administradores, empregados, prestadores de serviços e parceiros que possuam acesso a áreas, equipamentos, informações, redes e dados da JB3 SOFTWARES S.A.

3. Diretrizes

Todos os colaboradores devem estar preparados para identificar e notificar eventos e incidentes de segurança da informação e privacidade ou fragilidades observadas que possam causar:

Prejuízos;

Interrupções;

Maus funcionamentos;

Imprecisão;

Vazamento de dados nos sistemas e ambientes.

Todos os eventos de incidente de segurança da informação e privacidade devem ser registrados nos controles e/ou ferramentas para a devida triagem e tratamento;

Os eventos de incidente de segurança da informação e privacidade devem ser categorizados e classificados através de uma matriz de severidade com intuito de se ter uma melhor visibilidade, tratamento e prioridade quanto a sua gestão;

O conteúdo da notificação precisa ser claro, em formato simples e deve incluir as informações necessárias para a rápida e correta identificação do problema e da ação requerida;

Violações ou tentativas de violação da Diretriz de Segurança da Informação, de normas ou de controles de segurança da informação, intencionais ou não, são considerados incidentes de segurança.

Incidentes de segurança podem ser identificados por processos de monitoramento da área de infraestrutura por Colaboradores que observem fragilidades, anomalias e violações que coloquem a segurança da empresa em risco.

Vulnerabilidades ou fragilidades suspeitas não deverão ser objeto de teste ou prova pelos colaboradores, sob o risco de violar a política de segurança da informação, bem como provocar danos aos serviços ou recursos tecnológicos.

É de extrema importância que o horário de servidores e equipamentos de redes estejam sincronizados com uma fonte confiável de tempo (ex: via protocolo NTP) para que não haja disparidades na correlação de eventos, logs e outros dados.

Deve ser comunicado os incidentes de segurança da informação e privacidade de acordo com a severidade do incidente

4. Incidente de Segurança e Privacidade

São considerados Incidentes de Segurança da Informação e Privacidade quaisquer fragilidades ou eventos adversos de segurança, confirmados ou sob suspeita, que levem ou possam levar ao comprometimento de um ou mais dos princípios básicos de segurança da informação: confidencialidade, integridade, disponibilidade e conformidade, incluindo segurança física e proteção de ativos e colocando o negócio e seus objetivos em risco ou à imagem desta empresa.

Abaixo relacionamos alguns possíveis incidentes de segurança e privacidade, não se limitando:

Violações de políticas de segurança ou controles estabelecidos;

Perda ou corrupção de dados por desastres naturais;

Indisponibilidade por ataques maliciosos;

Vazamento ou roubo de informações;

Tentativas de acesso não autorizado;

Uso ou acesso indevido a dados ou sistemas;

Modificações não autorizadas em sistemas;

Tratamento incorreto de dados pessoais fora da finalidade declarada;

Descarte incorreto de documentos sigilosos, bem como compartilhamento inadequado de senhas pessoais;

Violação de acesso físico a áreas críticas;

Danos físicos intencionais a ativos da organização;

E, incidentes, falhas de infraestrutura ou ataques cibernéticos.

5. Definições

Segurança da Informação: Proteção da confidencialidade, integridade e disponibilidade das informações.

Incidente de Segurança da Informação: Evento que comprometa ou possa comprometer dados, sistemas ou serviços, bem como, a confidencialidade, integridade ou disponibilidade das informações.

Crise: Situação grave que afeta de forma significativa a operação, imagem ou a segurança de dados e requer ação coordenada imediata.

Plano de Continuidade das Operações (PCO): Estratégia e conjunto de procedimentos para garantir a manutenção ou rápida retomada das atividades críticas da organização após incidentes ou interrupções.

TRI – Time de Resposta a Incidentes: Equipe designada para investigar, mitigar, erradicar e registrar incidentes de segurança.

6. Princípios Gerais

Prevenção: Por meio de controles técnicos e administrativos visando implementar controles para reduzir a probabilidade de incidentes.

Detecção: Identificar de forma tempestiva qualquer evento anormal.

Resposta ágil: Atuar de maneira coordenada para conter danos e restaurar serviços.

Comunicação transparente: Informar as partes interessadas e autoridades competentes conforme exigido por lei.

Aprendizado contínuo: Incorporar lições aprendidas para aprimorar processos e controles.

7. Política de Segurança da Informação para Gestão de Crises

Durante a gestão de crises, especialmente as relacionadas à segurança da informação, a JB3 SOFTWARES S.A. adota os seguintes princípios e diretrizes adicionais:

Proteção da Informação

● Restringir o acesso a dados e sistemas críticos apenas a pessoal autorizado.

● Utilizar mecanismos de autenticação forte e segregação de funções.

● Implementar controles adicionais de monitoramento para detectar atividades anômalas.

Continuidade da Confidencialidade, Integridade e Disponibilidade

● Garantir que dados e serviços críticos sejam preservados durante a crise, com backups atualizados e redundâncias ativas.

● Utilizar canais seguros para comunicação interna e externa durante a crise.

● Proibir o uso de dispositivos ou redes não autorizados.

Gestão de Comunicação Segura

● Centralizar a comunicação oficial no Comitê de Crise.

● Garantir que todas as informações divulgadas sejam verificadas e autorizadas.

● Utilizar criptografia e ferramentas seguras para compartilhamento de dados.

Proteção contra Ameaças Internas e Externas

● Monitorar atividades suspeitas de usuários internos.

● Bloquear tentativas de acesso não autorizado.

● Reforçar controles contra ataques cibernéticos (DDoS, ransomware, phishing).

Registro e Auditoria:

● Registrar todas as ações tomadas durante a crise para posterior auditoria.

● Manter relatórios detalhados para análise pós-incidente.

8. Estrutura e Responsabilidades

Colaboradores: Reportar imediatamente incidentes ou suspeitas.

TRI – Time de Resposta a Incidentes: Avaliar, conter e erradicar incidentes, além de apoiar a recuperação.

Gestores: Disponibilizar recursos, apoiar a execução desta política e ações emergenciais.

DPO/Encarregado LGPD: Coordenar ações em casos envolvendo dados pessoais.

Comitê de Crise: Integrar representantes da alta direção, TI, jurídico e comunicação, responsável por decisões estratégicas em eventos de grande impacto.

9. Procedimentos de Resposta a Incidentes

Identificação do incidente.

Notificação ao canal oficial.

Classificação e determinação da gravidade (baixo, médio, alto, crítico).

Contenção com ações imediatas para impedir agravamento do impacto.

Erradicação e eliminação da causa raiz.

Recuperação e restauração segura dos serviços afetados.

Pós-incidente elaborar relatório de análise de impacto e medidas preventivas.

10. Comunicação de Incidentes

CANAL OFICIAL: seguranca@jb3ti.com.br.

Notificação às autoridades competentes, incluindo ANPD, TCU, CGU, MPF ou outros órgãos, no prazo legal ou contratual.

Comunicação aos titulares de dados, quando aplicável.

11. Gestão de Crises

O Comitê de Crise será acionado em eventos de alto impacto.

As ações incluem:

- Avaliação de riscos.
- Definição de estratégias emergenciais.
- Coordenação de comunicação com clientes, órgãos reguladores e imprensa.
- Priorização da continuidade dos serviços essenciais.

12. Plano de Continuidade das Operações (pco)

O PCO tem como finalidade assegurar que, em caso de interrupções, as operações críticas da JB3 SOFTWARES S.A. sejam mantidas ou retomadas no menor tempo possível.

Identificação de processos críticos: Listagem dos serviços e sistemas essenciais para o negócio.

Análise de Impacto nos Negócios (BIA): Avaliação dos efeitos de interrupções prolongadas.

Definição de RTO/RPO:

- RTO (Recovery Time Objective) – tempo máximo para restabelecer o serviço.
- RPO (Recovery Point Objective) – perda máxima aceitável de dados.

Recursos de contingência:

- Backup diário de dados.
- Redundância de servidores e links de internet.
- Serviços em nuvem para mitigação de falhas físicas.

Procedimentos de recuperação: Passo a passo para retorno seguro das operações.

Testes periódicos: Simulações semestrais para validar o PCO.

Plano de comunicação de crise: Roteiro para informar clientes, parceiros e órgãos reguladores sobre a situação e medidas adotadas.

13. Treinamento e Conscientização

Treinamentos anuais obrigatórios sobre segurança da informação e gestão de crises para os colaboradores.

Simulações práticas de incidentes e crises para aprimorar as respostas e o PCO.

14. Revisão e Atualização

Esta política será revisada anualmente ou após incidentes relevantes. Alterações devem ser aprovadas pela alta direção da JB3 SOFTWARES S.A.

15. Vigência

Esta política entra em vigor na data de sua aprovação e revoga quaisquer versões anteriores.

16. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
POLÍTICA DE GESTÃO DE CRISES, RESPOSTAS A INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E PLANO DE CONTINUIDADE DAS OPERAÇÕES	Manual de Procedimentos	30/04/2025	1.0

Data	Descrição Ação	Versão	Responsável
30/04/2025	Elaboração	1.0	Jurídico
30/04/2025	Revisado e Aprovado	2.0	Diretoria Executiva

1. Objetivo

A GCC possui mecanismos para gerar e gerenciar hash criptográficos únicos, assegurando:
• Integridade dos dados, evitando alterações não autorizadas.
• Autenticidade e rastreabilidade, permitindo validação segura de informações e transações.
• Proteção contra fraudes, por meio de algoritmos robustos e irreversíveis (ex.: SHA256).
• Gestão eficiente, com controle sobre criação, armazenamento e verificação dos hashes.
• Conformidade com padrões de segurança, garantindo aderência às melhores práticas e normas regulatórias.

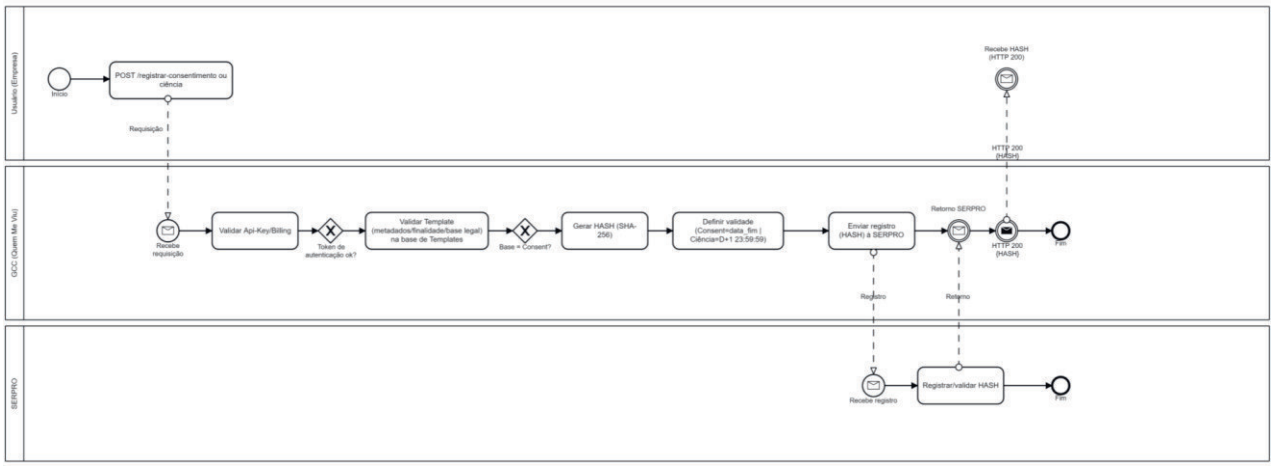
2. Controle do Hash

O hash gerado pela GCC é compatível com os padrões exigidos e utiliza o algoritmo SHA-256, reconhecido internacionalmente por sua robustez e confiabilidade. Benefícios:
• Alta segurança: SHA-256 é um algoritmo irreversível, dificultando ataques de força bruta e garantindo integridade dos dados.
• Conformidade com normas: Atende aos padrões exigidos por regulamentações e boas práticas de segurança.
• Proteção contra fraudes: Garante que dados não sejam alterados sem detecção.
• Escalabilidade e interoperabilidade: Pode ser aplicado em diferentes sistemas e processos sem comprometer desempenho.
• Rastreabilidade confiável: Permite validação segura de transações e informações.

Exemplo do modelo de concatenação dos dados:
• Data e hora do pedido do Hash (request)
• Data e hora do response do Hash (geração)
• Tipo de Pessoa: PF ou PJ
• CPF/ CNPJ Titular
• ID Template
• Consentimento: True ou False
• CNPJ do requerente (usuário)
• CNPJ Anuente
• CNPJ GCC
• Código de transação
• Data do pedido do consentimento
• Data da autorização do consentimento (Data início)
• Data Expiração Hash (data fim consentimento)/quando for ciência 24 horas

3. BPMN Fluxo de registro de consentimento e ciência

O BPMN (Business Process Model and Notation) abaixo demonstra a forma padronizada e visual do fluxo de registro de consentimento e ciência onde ocorre a geração do HASH.

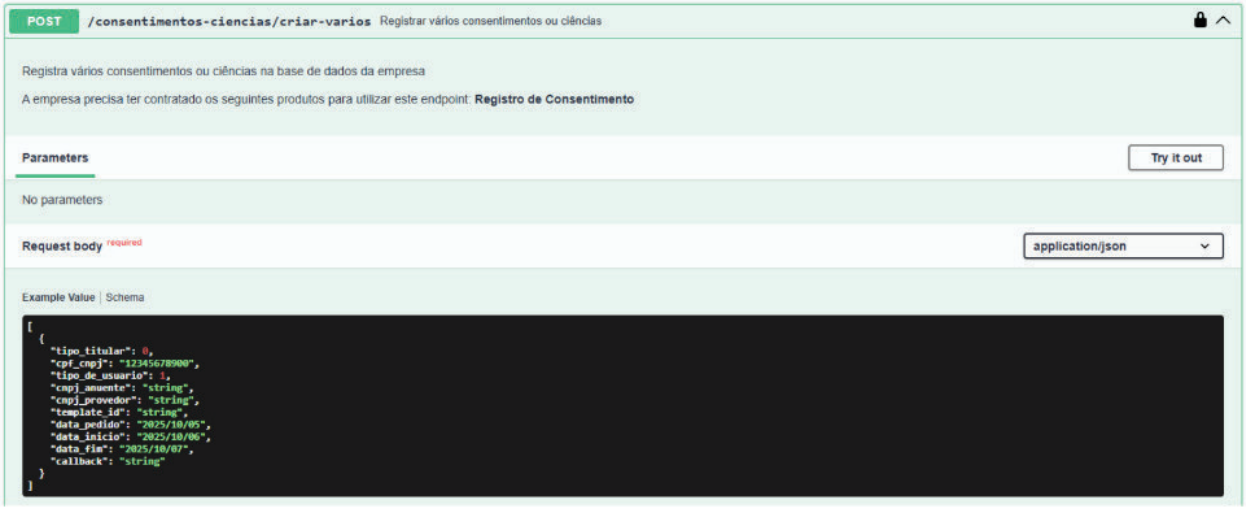


4. Capacidade gerar arquivos batch

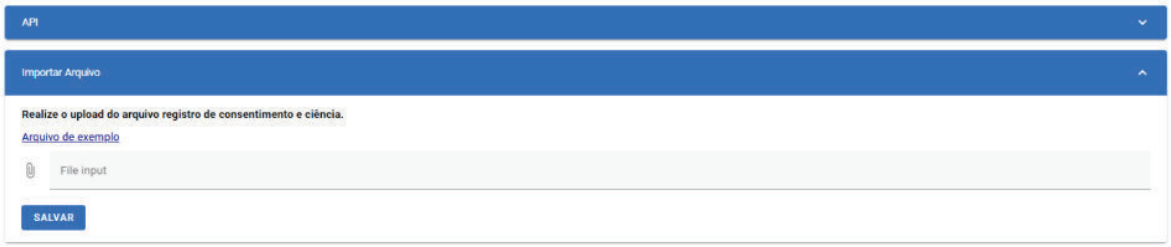
A principal vantagem da solução da GCC ao permitir a geração de arquivos batch é a automação e padronização de processos repetitivos, trazendo ganhos significativos em eficiência operacional.

Exemplo via API

O endpoint /consentimentos-ciencias/criar-varios possibilita incluir vários registros, independente da base legal ou tipo de pessoa (PF/PJ), de uma única vez por meio de lista.



Exemplo plataforma de usuário empresa (clientes)
Possibilitamos aos usuários os registros de consentimentos e ciências via arquivo através da plataforma de empresa, área integrações.
URL https://plataforma.hml.quemmeviu.com.br/empresa/login

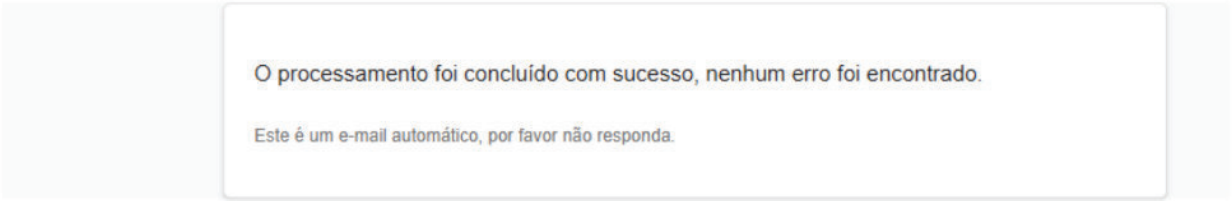


Arquivo exemplo

	A	B	C	D	E	F	G	H	I
1	tipo_titular	cpf_cnpj	tipo_usuario	cnpj_anuente	cnpj_provedor	template_id	data_pedido	data_inicio	data_fim
2	1	000.000.000-01	1		00.000.000/0000-03	100	21/10/2025	22/10/2025	23/10/2025
3	2	00.000.000/0000-01	2	00.000.000/0000-02	00.000.000/0000-03	200	18/10/2025	21/10/2025	21/10/2025
4									
5									
6									

Acompanhamento do processamento via e-mail

Para: polyana.silva+1@jb3ti.com.br



5. Histórico de alterações

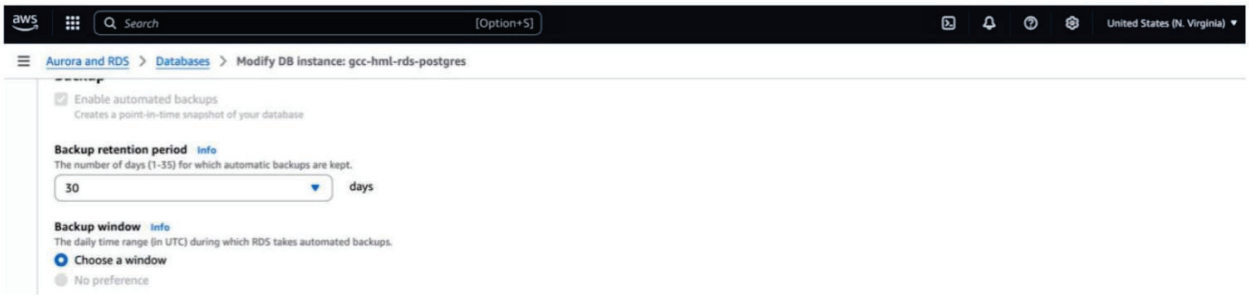
VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

1. Descrição

A gerenciadora de consentimentos e ciências possui mecanismos de registro e rastreabilidade para todas as ações realizadas nas plataformas e apis.

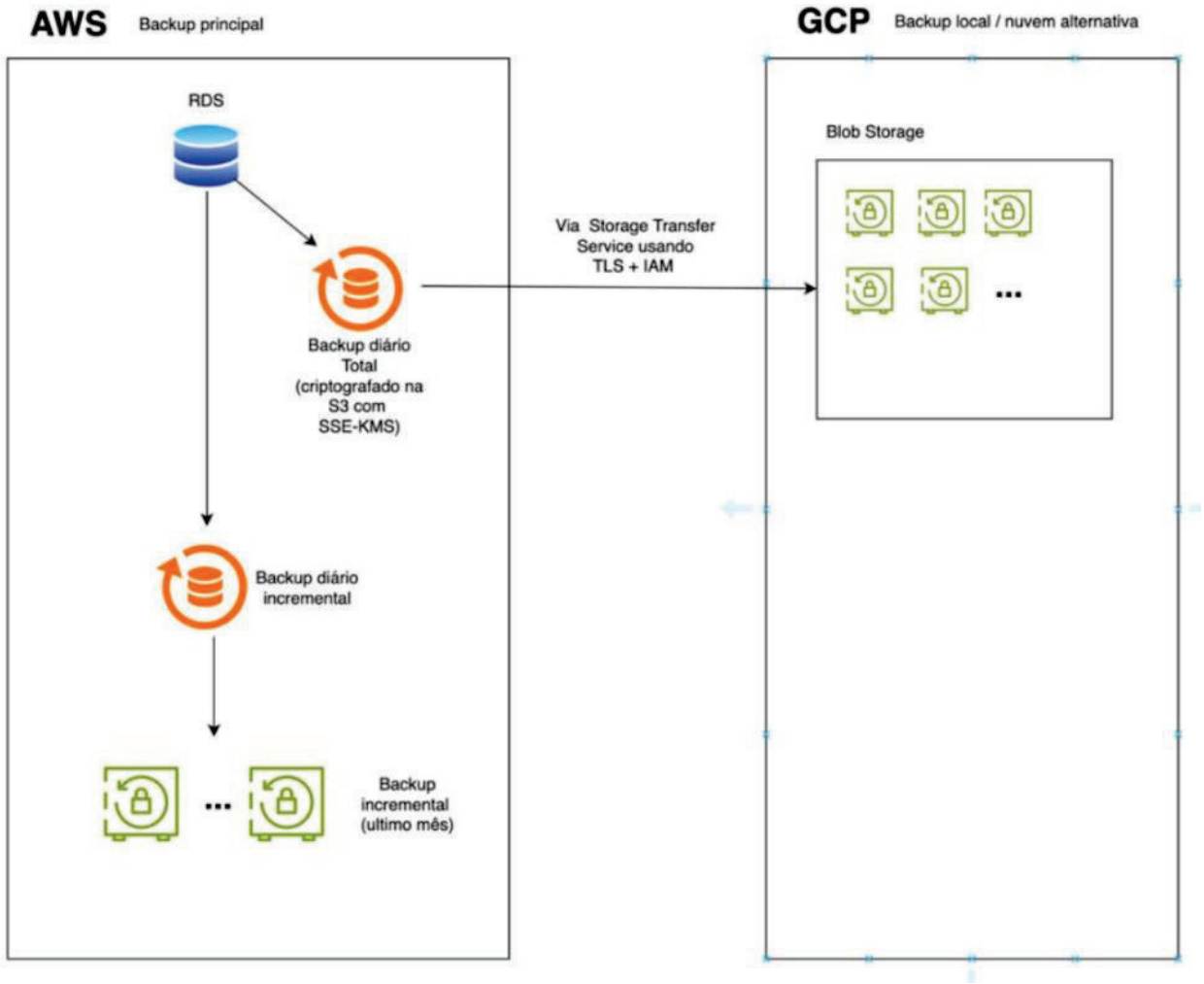
2. Backup com duplo local de armazenamento

A plataforma possui sistema de backup alternativo ao da cloud principal (duplo local de armazenamento). O backup principal encontra-se implementado na cloud principal da solução (AWS), onde o backup é feito de forma incremental diária de modo automático, garantindo um full backup (backup total) mínimo mensal.



O backup duplo encontra-se localizado numa cloud secundaria (GCP) onde a cópia do full-backup (backup total) é feita de forma diária.

O backup efetuado é criptografado com SSE-KMS e todo o seu transporte também é encriptado usando TLS e IAM para autenticação.

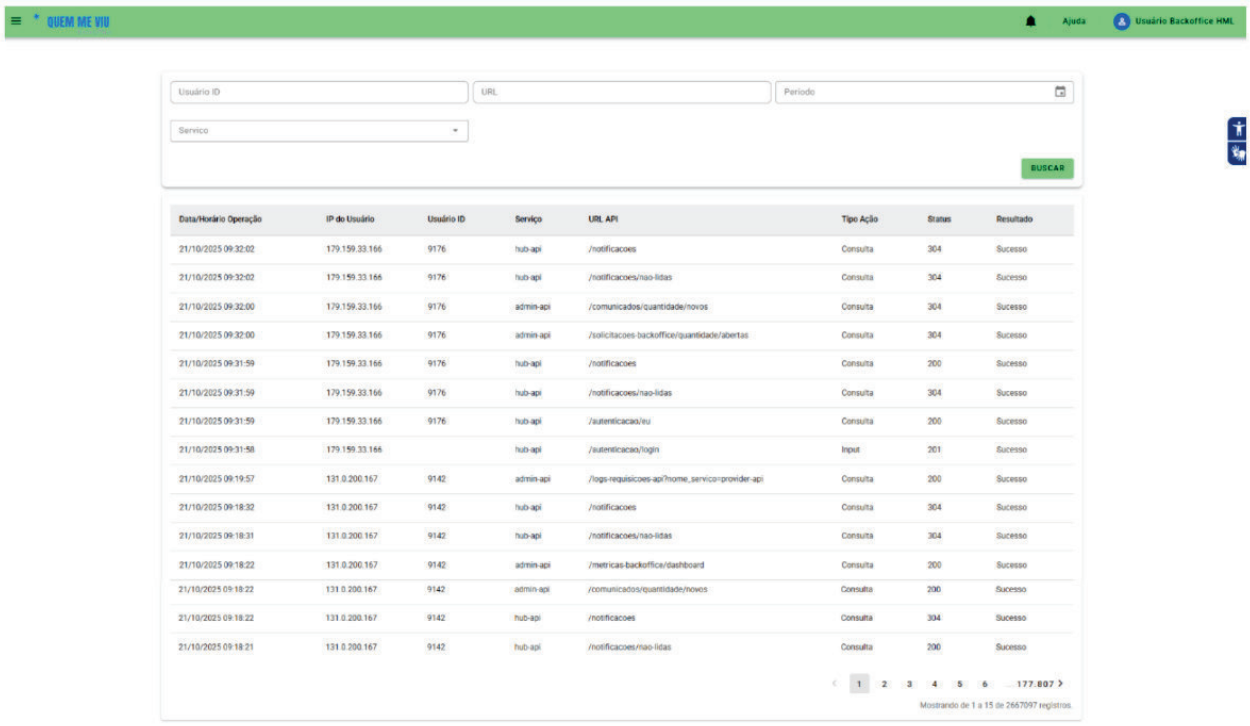


3. Logs de acesso

Manter logs de acesso é essencial para:

• Rastreabilidade: Identificar quem acessou, quando e de onde, garantindo transparência.
• Segurança: Detectar acessos indevidos e prevenir incidentes.
• Auditoria e conformidade: Atender requisitos regulatórios (LGPD, ISO 27001) e fornecer evidências em auditorias.
• Monitoramento e análise: Permitir diagnóstico de falhas e melhoria contínua.
• Responsabilidade: Assegurar que todas as ações sejam atribuíveis a usuários específicos. Na plataforma do BackOffice é possivel ter acesso aos Logs de acesso que contemplam data/horário operação, IP do usuário, Usuário (ID), Serviço, URL da API, Tipo de ação, Status e Resultado.

https://plataforma.hml.quemmeviu.com.br/admin/login



4. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

1. OBJETIVO

Descrever como a JB3 SOFTWARES S.A. atende os requisitos de implantação, operação, monitoramento, revisão, manutenção e melhoria do Sistema de Gestão Integrado conforme as normas ISO/IEC 9001, 27001, 27018, 27701 e 42001 em sua versão atual, considerando o contexto da organização e as questões internas e externas que apoiam seu negócio.

2. VIGÊNCIA

Este Manual passa a vigorar a partir da data da sua publicação.

3. DEFINIÇÕES

- **LGPD:** Lei Geral de Proteção de Dados Pessoais.
- **SGI:** Sistema de Gestão Integrado.

4. DOCUMENTOS RELACIONADOS

POL.000 - Política Integrada

POL.001 - Política de Segurança da Informação

POL.008 - Política de Privacidade e Proteção de Dados

5. CONTEXTO DA ORGANIZAÇÃO

5.1. Entendendo a Organização e seu Contexto

As questões internas e externas que são relevantes para o seu propósito e que afetam sua capacidade para alcançar os resultados pretendidos do seu SGI estão destacadas nos tópicos a seguir:

	Pontos Fortes	Pontos Fracos
Ambiente Interno	Produto customizável, ajustável as necessidades. Comprometimento com a entrega através de SLAs estabelecidos em contrato.	Equipe enxuta, dependência de pessoas e sobrecarga de trabalho. Cultura de Segurança da Informação e Privacidade em desenvolvimento. Governança, empresa recém-inaugurada com processos em desenvolvimento.

	Oportunidades	Ameaças
Ambiente Externo	A contínua inovação nos produtos pode impulsionar a empresa no mercado. Desenvolvimento de novos produtos e serviços, com a avaliação de privacidade desde a concepção do produto.	Novas ou atualizações das legislações, portarias e/ou novas diretrizes aplicáveis. Situação Política, Social e Econômica do país As mudanças climáticas podem afetar a continuidade dos negócios, forçando adaptações nos sistemas de gestão da qualidade, segurança da informação e privacidade, devido a possíveis interrupções nas operações e a necessidade de atender a novas regulamentações ambientais.

As mudanças realizadas em ambas as questões serão tratadas no FOR.002 – Ata de Reunião, revisado anualmente e criticamente pela Alta Direção.

Importante: A JB3 SOFTWARES S.A. analisou as questões relacionadas as mudanças climáticas como secas, inundações, estresse térmico, aumento das temperaturas, aumento do nível do mar, ondas de calor e não identificou que possa sofrer algum impacto e com relação ao que ela possa impactar, algumas ações são tomadas como trabalho remoto, sem deslocamento dos envolvidos, previsão de descarte seguro que equipamentos, quando necessário.

5.2. Entendendo as Necessidades e Expectativas das Partes Interessadas

A organização entende as necessidades e expectativas das partes interessadas na forma apresentada a seguir:

Partes Interessadas	Necessidade / Expectativa	Monitoramento
Clientes	• Garantia da confidencialidade, integridade, disponibilidade e privacidade das informações. • Parceiro de negócios capaz de entender suas necessidades de segurança da informação, privacidade e infraestrutura de TI traduzidos em produtos e serviços de qualidade a preços competitivos. • Expectativas crescentes por inovações e qualidade.	• Pesquisa de Satisfação de Clientes • Práticas de Segurança da Informação e Privacidade
Direção	• Garantia da segurança do sistema e das informações dos clientes e colaboradores da empresa. • Atendimento aos requisitos de contrato. • Gestão da continuidade do negócio. • Sustentabilidade da organização e lucratividade anual de acordo com as metas de resultados definidas.	• Práticas de Segurança da Informação e Privacidade • Acompanhamento de Indicadores
Colaboradores	• Processos estruturados e documentados. • Infraestrutura e ambiente de trabalho adequados. • Garantia da confidencialidade, integridade, disponibilidade e privacidade das informações. • Remuneração compatível com o mercado de trabalho, ambiente de crescimento e desenvolvimento profissional e pessoal, participação nos lucros anuais. • Necessidade de um ambiente de trabalho motivador e oportunidades de crescimento.	• Formalização de processos e revisões periódicas. • Práticas de Segurança da Informação e Privacidade
Fornecedores	• Garantia da confidencialidade, integridade, disponibilidade e privacidade das informações. • Gestão da continuidade do negócio. • Estabilidade nas relações comerciais e qualidade dos insumos.	• Monitoramento do contrato • Práticas de Segurança da Informação e Privacidade
Órgãos governamentais	• Atendimento das leis pertinentes e aplicáveis, e recolhimento dos tributos devidos. • Cumprimento de normas e regulamentos do setor.	• Acompanhamento periódico da legislação aplicável.
Titular de Dados Pessoais	• Proteção contra acessos não autorizados. • Transparência no tratamento de dados. • Controles sobre as informações coletadas e armazenadas. • Consentimento informado.	• Práticas de Segurança da Informação e Privacidade
Autoridade Nacional de	• Estabelecimento de padrões para garantir que dados pessoais sejam protegidos contra acessos indevidos, vazamentos e uso abusivo.	• Gestão dos incidentes de privacidade

Proteção de Dados - ANPD	• Criação de normas claras para a aplicação da LGPD e fiscalizar o cumprimento da legislação por empresas e órgãos públicos.	

Importante: Para o escopo da certificação, não foram identificadas necessidades ou expectativas das partes interessadas relacionadas as mudanças climáticas como secas, inundações, estresse térmico, inundações, aumento das temperaturas, aumento do nível do mar, ondas de calor e não identificou que possa sofrer algum impacto e com relação ao que ela possa impactar.

Os requisitos das partes interessadas serão revisados anualmente e criticamente pela Alta Direção ou quando for necessário e documentado no FOR.002 – Ata de Reunião.

5.3. Determinando o Escopo do SGI

A JB3 SOFTWARES S.A. atua no mercado de tecnologia ofertando software o qual entrega ao segmento interessado em consumir dados do SENATRAN consulta de informações junto ao órgão público. Para o titular do dado, a plataforma entrega uma solução para acompanhamento do consentimento e ciência às empresas devidamente homologadas junto ao Senatran, conforme Portaria 139. Essa solução será utilizada por seus clientes com alto nível de controle e gerenciamento da infraestrutura, segurança da informação, sistemas e instalações de TI relacionadas e demais processos intrínsecos ao seu desenvolvimento e manutenção.

Conforme descrito acima, a organização determinou os limites e a aplicabilidade do SGI para estabelecer o seu escopo, de acordo com as questões internas, externas e perspectivas das partes interessadas nas atividades que realiza:

ISO 9001:2015

O Sistema de Gestão de Qualidade no Processo B2B – Desenvolvimento de software e suporte.

Exclusão

- **Item 7.1.5 – Recursos de monitoramento e medição**
  - Os requisitos relacionados ao item não são aplicáveis ao escopo do Sistema de Gestão Integrado uma vez que não há atividades ou áreas que utilizem de equipamentos de calibração para realizar medição de equipamentos e ambientes.

ISO 27001:2022

O Sistema de Gestão de Segurança da Informação no Processo B2B – Desenvolvimento de software e suporte - conforme DOC.006 - Declaração de aplicabilidade v.4.0 de 15/08/2025."

ISO 27018:2019

"Proteção de dados pessoais em nuvem no Processo B2B – Desenvolvimento de software e suporte - conforme DOC.006 - Declaração de aplicabilidade v.4.0 de 15/08/2025."

ISO 27701:2019

O Sistema de Gestão de Privacidade da Informação no Processo B2B – Desenvolvimento de software e suporte - conforme DOC.006 - Declaração de aplicabilidade v.4.0 de 15/08/2025."

ISO 42001:2023

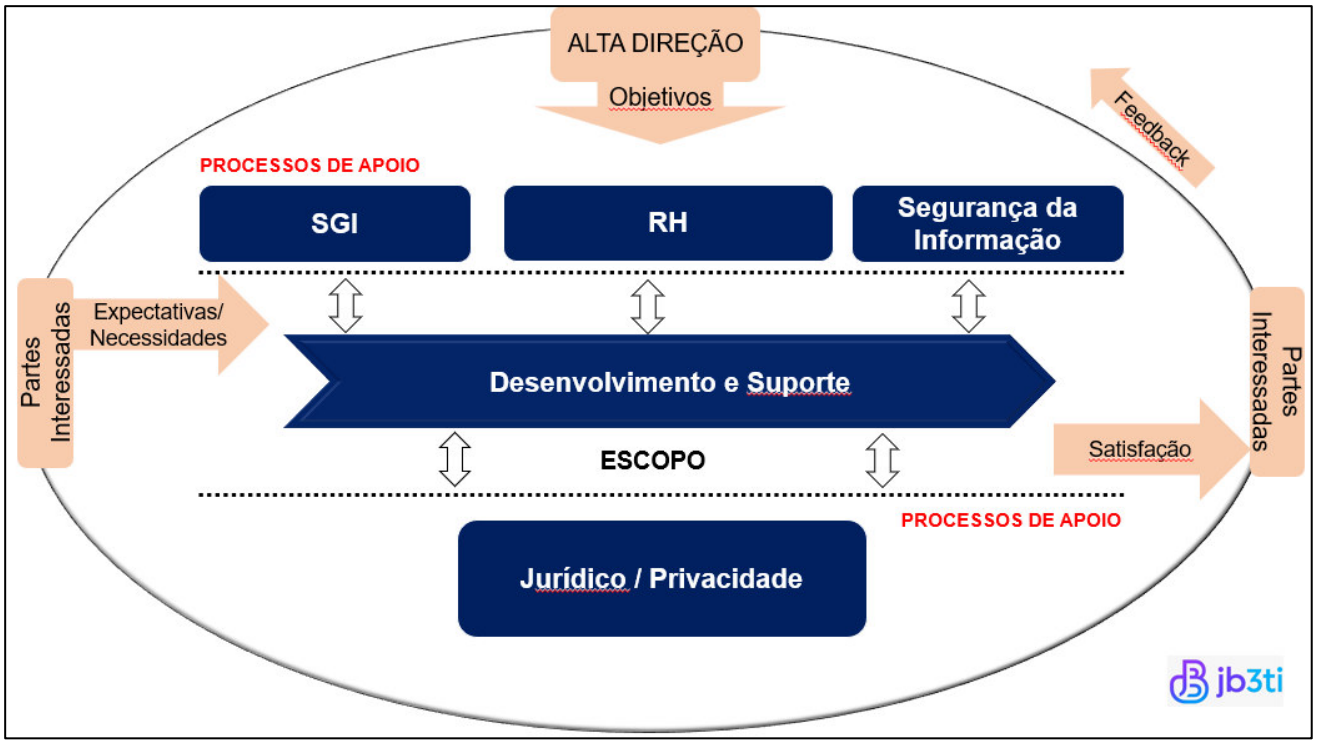
O Sistema de Gestão da Inteligência Artificial com base na ISO 42001:2023 – no Processo B2B – Desenvolvimento de software e suporte - conforme DOC.006 - Declaração de aplicabilidade v.4.0 de 15/08/2025."

Localidade: Avenida Paulista, 2300 - Piso Pilotis - Sala 43 – Ed. São Luís Gonzaga - Consolação - São Paulo/SP CEP:01310-300

***Operador:** para os dados pessoais das demandas.

5.4. SGI

A JB3 SOFTWARES S.A. estabelece, implementa, mantem e melhora continuamente um SGI, incluindo os processos necessário e suas interações, de acordo com os requisitos deste Manual. Abaixo temos uma visão macro e no DOC.010 - Mapeamento de Processos é possível verificar o detalhamento dos processos e suas interações.



6. LIDERANÇA

6.1. Liderança e Comprometimento

6.1.1. Comprometimento

A Alta Direção da JB3 SOFTWARES S.A., através demonstra sua liderança e comprometimento em relação ao SGI pelos seguintes meios:

a) Assegurando que a Política de Segurança da Informação e os objetivos de segurança da informação estejam estabelecidos e sejam compatíveis com a direção estratégica da organização, assim como a Política e os objetivos de Privacidade;

b) Assegurando a integração dos requisitos do SGI nos processos da organização, conforme descrito no item **6.3. Autoridades, Responsabilidades e Papéis Organizacionais** deste Manual;

c) Assegurando que os recursos necessários para o SGI estejam disponíveis;

d) Comunicando a importância de uma gestão eficaz da segurança da informação e da conformidade com os requisitos do SGI;

e) Assegurando que o SGI alcance os seus resultados pretendidos;

f) Orientando e apoiando pessoas a contribuir para a eficácia do SGI;

g) Promovendo a melhoria contínua, conforme definido no item **11. MELHORIA** deste Manual;

h) Apoiando outros papéis relevantes da gestão para demonstrar como sua liderança se aplica as áreas sob sua responsabilidade.

6.1.2. Foco no cliente

A alta direção da JB3 SOFTWARES S.A. demonstra liderança e comprometimento com o foco no cliente ao assegurar que os requisitos dos clientes, bem como os requisitos estatutários e regulamentares aplicáveis, sejam continuamente determinados, compreendidos e atendidos. Além disso, são identificados e tratados os riscos e oportunidades que possam impactar a conformidade dos produtos e serviços ou a capacidade de aumentar a satisfação dos clientes. A JB3 SOFTWARES S.A. mantém como prioridade estratégica a busca pela excelência no atendimento, promovendo ações que visam não apenas satisfazer, mas superar as expectativas dos clientes, fortalecendo a confiança e a fidelização. Para apoiar nesse engajamento a JB3 SOFTWARES S.A. realiza Pesquisa de Satisfação em cliente pelo menos uma vez a cada 12 meses.

6.2. Política

A Alta Direção da JB3 SOFTWARES S.A. estabeleceu a POL.010 - Política Integrada, POL.001 - Política de Segurança da Informação e POL.008 - Política de Privacidade e Proteção de Dados apropriada ao propósito da organização, incluindo os objetivos do sistema de gestão. Foram documentadas, comunicadas e estão disponíveis às partes interessadas, quando apropriado.

6.3. Papéis, Responsabilidades e Autoridades Organizacionais

A Alta Direção da organização assegura que as responsabilidades estão definidas na POL.001 - Política de Segurança da Informação e nas demais Políticas e Procedimentos estabelecidos, quando aplicável.

As autoridades dos papéis relevantes para a segurança da informação são atribuídas e comunicadas na POL.001 - Política de Segurança da Informação, DOC.005 – Matriz RACI e no DOC.004 - Organograma disponibilizado no repositório padrão.

7. PLANEJAMENTO

7.1. Avaliação de impacto, Avaliação e Tratamento de Riscos e Oportunidades

A organização considerou para o planejamento do SGI as questões referenciadas no item **5.1. Entendendo a Organização e seu Contexto** e os requisitos descritos no item **5.2. Entendendo as Necessidades e Expectativas das Partes Interessadas** deste Manual, para determinar os riscos e oportunidades que precisam ser consideradas para assegurar que o SGI possa alcançar seus resultados pretendidos, prevenir ou reduzir os efeitos indesejados e alcançar a melhoria contínua, conforme apresentado no DOC.001 – Gestão de Riscos e Oportunidades, que estabelece:

- Os critérios de riscos;
- Os critérios de aceitação do risco;
- Os critérios para o desempenho das avaliações dos riscos e análise de impacto.

A organização define e aplica um processo de tratamento dos riscos do SGI para selecionar, de forma apropriada, as opções de tratamento dos riscos, levando em consideração os resultados da avaliação do risco, conforme definido no DOC.001 – Gestão de Riscos e Oportunidades.

Os controles necessários para implementar as opções escolhidas do tratamento do risco da segurança da informação e privacidade estão definidas no DOC.001 - Gestão de Riscos e Oportunidades e devem ser monitorados até a próxima avaliação dos riscos.

A organização compara os controles determinados no DOC.001 – Gestão de Riscos e Oportunidades com aqueles definidos no DOC.006 – Declaração de Aplicabilidade, com a justificativa para inclusões, sejam eles implementados ou não, bem como a justificativa para a exclusão dos controles.

Os riscos são reavaliados anualmente e aprovados pela Alta Direção, porém, novos riscos poderão ser identificados a qualquer momento.

7.2. Objetivos da Segurança da Informação, Privacidade e o Planejamento Para Alcançá-los

A organização estabelece os objetivos para o seu sistema de gestão para as funções e níveis relevantes na POL.010 - Política Integrada, POL.001 - Política de Segurança da Informação, POL.008 - Política de Privacidade e Proteção de Dados e planos de ação serão definidos com o objetivo de alcançar os resultados esperados.

Objetivo	Medição / monitoramento	Periodicidade	Meta	O que será feito	Quais recursos necessários	Quem será responsável	Processo atrelado	Quando estará concluído	Como os resultados serão avaliados
Aumentar a Satisfação do Cliente	Satisfação dos clientes.	Anual	90% dos clientes satisfeitos com a prestação de serviço	Elaboração uma pesquisa de satisfação sobre os produtos e serviços ofertados pela JB3 SOFTWARES S.A.	Ferramenta office	Analista de Segurança da Informação	Desenvolvimento e Suporte	Contínuo	Índice de satisfação dos clientes e possíveis reclamações
Garantir a conformidade com as normas ISO 27001 e ISO 27701, além de outras leis e regulamentos aplicáveis à proteção de dados.	Número de não conformidades identificadas em auditoria externa	Anual	100% dos planos de ação tratados (Auditoria Externa)	Elaboração da Ata de Análise Crítica pela Direção e Planos de Ação identificados	Os recursos estarão especificados em cada Plano de Ação, descrito na Ata de Análise Crítica	Analista de Segurança da Informação	Segurança da Informação	Contínuo Após implementação e avaliação de eficácia do plano de ação	Planos de Ação concluídos e avaliação de eficácia avaliada
Manter a confidencialidade, integridade e disponibilidade da informação.	Número de incidentes de segurança	Mensal	NA	Análise dos incidentes de segurança	Ferramenta office	Analista de Segurança da Informação	Segurança da Informação	Contínuo	Número de Incidentes de Segurança da Informação tratados

Proteger a informação, evitando vazamentos e acessos não autorizados.	Número de incidentes de privacidade de dados	Mensal	NA	Análise dos incidentes de privacidade de dados	Ferramenta office	Analista de Segurança da Informação	Segurança da Informação	Contínuo	Número de Incidentes de Privacidade de Dados, reportados e tratados
Implementar um processo de melhoria contínua do SGI, com base em avaliações de riscos e análises de incidentes	Matriz de Riscos revisadas pelos Gestores	Anual	100% dos riscos analisados	Elaboração da Ata de Análise Crítica pela Direção e Planos de Ação das melhorias identificadas	Os recursos estarão especificados em cada Plano de Ação para tratamento dos Riscos	Analista de Segurança da Informação	Todos os processos	Contínuo	Quantidade de Riscos tratados / Quantidade Total de Riscos Identificados
A capacitação profissional deve ser realizada com objetivo de manter e melhorar o nível de segurança da informação.	Conscientização de Segurança de Informação	Anual	100% dos colaboradores capacitados	Comunicações online e treinamento no Onboarding e requalificação pelo menos uma vez ao ano	Ferramenta office	Analista de Segurança da Informação	RH	Contínuo	Número de colaboradores concientizados / Número de total de colaboradores

7.3. Planejamento de mudanças

A JB3 SOFTWARES S.A. estabelece que mudanças significativas no sistema de gestão integrado através do processo de mudança, conforme estabelecido no PRO.006 - Gestão de Mudança.

8. APOIO

8.1. Recursos

A organização determina e provê recursos necessários para o estabelecimento, implementação, manutenção e melhoria contínua do SGI. Anualmente, a Alta Direção elabora um plano de investimento conforme o FOR.006 - Plano de Investimento.

Através do processo de seleção e contratação estabelecido e treinamentos providos internamente, a JB3 SOFTWARES S.A. garante a aderência ao Sistema de Gestão.

A JB3 SOFTWARES S.A. garante a infraestrutura necessária a seus colaboradores e demais partes interessadas, conforme aplicável, para alcançar a conformidade de seus produtos e serviços. Todas as atividades realizadas pela JB3 SOFTWARES S.A. ocorrem de maneira remota.

8.2. Competência

A organização determina a competência necessária das pessoas que realizam trabalhos sob o seu controle e que afeta o desempenho do sistema de gestão, conforme estabelece o DOC.014 – Descrição de Cargo.

8.3. Conscientização

As pessoas que realizam trabalhos sob o controle da organização são conscientizadas em relação as políticas, de acordo com suas contribuições para a eficácia do SGI, incluindo os benefícios da melhoria do desempenho e implicações da não conformidade com os requisitos do SGI.

8.4. Comunicação

A organização deve determinar as comunicações internas e externas relevantes para o SGI no DOC.003 - Plano de Comunicação.

8.5. Informação Documentada

Cada informação criada dentro da JB3 SOFTWARES S.A. deve ter um proprietário, que pode ser uma pessoa ou um departamento. Esse proprietário deve identificar quem serão os usuários da informação gerada, o nível de sigilo necessário e, com base nesses fatores, classificar a informação como:

Pública - Nível de sigilo baixo ou inexistente. Qualquer pessoa pode ter acesso à informação.

Interna - Nível de sigilo médio. Apenas os colaboradores da JB3 SOFTWARES S.A. podem ter acesso à informação.

Confidencial - Nível de sigilo alto. Apenas um grupo restrito de colaboradores da JB3 SOFTWARES S.A. pode ter acesso à informação.

Todas as informações devem ser devidamente classificadas e conter sua classificação em local visível. Documentos em formato digital ou impresso, classificados como confidenciais, devem ser rotulados de maneira que esta informação esteja visível desde o primeiro contato do usuário com o mesmo.

Os usuários com acesso a informações classificadas como confidenciais não devem divulgar tais informações, salvo mediante autorização por escrito do proprietário e/ou do Analista de Segurança da Informação.

O acesso a informações confidenciais deve ser concedido pelo proprietário com base no Need-to-Know (princípio de que as informações só devem ser acessadas por aqueles cuja necessidade de acesso seja justificável).

Os acordos de confidencialidade são renovados bianualmente através do formulário enviado aos colaboradores.

Todos os documentos gerados devem seguir os padrões de documentação que foram elaborados, estes templates foram criados para servir de base na elaboração de procedimentos, políticas, formulários, instruções operacionais e demais documentos a serem utilizados no Sistema de Gestão de Segurança da Informação e Privacidade, de acordo com PRO.001 – Procedimento de Controle de Documentos.

A organização controla o acesso pelas permissões dos diretórios e revisão da informação documentada no repositório padrão.

9. OPERAÇÃO

9.1. Planejamento e Controle Operacionais

A organização planeja, implementa e controla os processos necessários para atender os requisitos requeridos pelos sistemas de gestão implementados.

A organização mantém a informação documentada na abrangência necessária para gerar confiança de que os processos estão sendo realizados conforme planejado, bem como controla as mudanças planejadas e analisa criticamente as consequências de mudanças não previstas, tomando ações para mitigar quaisquer efeitos adversos. São considerados:
- Mudanças de processos – FOR.007 – Plano de Ação
- Mudanças de TI – PRO.006 – Gestão de Mudanças
- Monitoramento – FOR.028 – Avaliação de Eficácia dos Controles

A organização assegura que os processos terceirizados estão determinados e são controlados, conforme estabelece a POL.010 - Política Integrada, POL.006 – Política de Segurança da Informação e Privacidade para Fornecedores.

9.2. Avaliação de Riscos do Sistema de Gestão

A organização realiza avaliações de riscos do sistema de gestão com a periodicidade, no mínimo a cada 12 meses e quando mudanças significativas são propostas ou ocorrem. A organização retém a informação documentada dos resultados das avaliações de risco de segurança da informação no DOC.001 – Gestão de Riscos e Oportunidades.

9.3. Tratamento de Riscos do Sistema de Gestão

A organização implementa o plano de tratamento de riscos do sistema de gestão, conforme definido no DOC.001 – Gestão de Riscos e Oportunidades.

9.4. Avaliação de impacto do Sistema de Gestão

A organização identifica e documenta os impactos relacionados aos riscos identificados no DOC.001 – Gestão de Riscos e Oportunidades.

9.5. Requisitos para produtos e serviços

A JB3 SOFTWARES S.A. planeja e desenvolve os processos necessários para a realização do produto. O planejamento da realização do produto é coerente com os requisitos de outros processos do Sistema de Gestão Integrado:

- Objetivos da Qualidade e requisitos para o produto;
- A necessidade de estabelecer processos, documentos e prover recursos específicos para o produto;
- Verificação, validação, monitoramento bem como os critérios de aceitação do produto/serviço, e
- Registros necessários para fornecer evidência de que os processos de realização e o produto resultante atendem aos requisitos.

9.5.1. Comunicação com o cliente

A JB3 SOFTWARES S.A. determina e toma providências eficazes para se comunicar com os clientes sobre produto, serviços, consultas, contratos e realimentação do cliente, realizada pelos canais de atendimento (telefone, e-mail e presencial), sejam informações, pedidos, reclamações ou temas ligados à necessidade do cliente. A JB3 SOFTWARES S.A. também mantém seu site www.JB3.com.br que garante a possibilidade de seus clientes ou clientes em potencial se comunicarem com a empresa para informações sobre produtos e serviços.

A JB3 SOFTWARES S.A. assegura que a comunicação interna relativa aos processos do Sistema de Gestão é efetiva pelos comunicados internos, instruções no local de trabalho, reuniões, e-mails, dentre outros.

9.5.2. Determinação de requisitos relativos a produtos e serviços

A JB3 SOFTWARES S.A. determina:

- Os requisitos especificados pelo cliente, incluindo os requisitos para entrega e para atividades de pós-entrega;
- Os requisitos não declarados pelo cliente, mas necessários para o uso especificado ou intencional, onde conhecido;
- Requisitos estatutários e regulamentares relacionados ao produto, e
- Requisitos adicionais, determinados pela própria JB3 SOFTWARES S.A.

O Jurídico é responsável por identificar novos requisitos e adequar a empresa às novas exigências, atender as solicitações legais já existentes, atentar a impactos causados por atualizações aos requisitos já atendidos. As normas e leis identificadas como requisitos pelas JB3 SOFTWARES S.A. são relacionadas FOR.003 - Controle de Leis e Documentos.

Os requisitos relacionados a produtos são determinados e expressados nas propostas técnicas e comerciais da JB3 SOFTWARES S.A.

9.5.3. Análise Crítica dos Requisitos Relacionados ao Produto

A JB3 SOFTWARES S.A. analisa criticamente os requisitos relacionados ao produto ou serviço. Esta análise crítica é realizada antes da JB3 SOFTWARES S.A. assumir o compromisso de fornecer um produto para o cliente e assegura que:

- Os requisitos do produto estão definidos;
- Os requisitos de contrato ou de pedido que diferem daqueles previamente manifestados são resolvidos, e
- A JB3 SOFTWARES S.A. tem a capacidade para atender aos requisitos definidos.

Quando os requisitos do produto forem alterados, a JB3 SOFTWARES S.A. assegura que os documentos pertinentes são complementados e que o pessoal pertinente é alertado sobre os requisitos alterados em suas propostas ou contratos.

As análises críticas dos requisitos relativos a produtos e serviços são realizadas sob demanda ou pelo menos uma vez a cada 12 (doze) meses para garantir a aderência ao processo. Registros destas análises críticas de produto/serviço devem ser mantidos.

9.5.4. Mudanças nos requisitos para produtos e serviços

Para todas as alterações que ocorrerem relacionadas as mudanças nos requisitos dos produtos e serviços devem ser documentadas e os colaboradores envolvidos são alertados sobre os requisitos que foram mudados. Os meios pelos quais os envolvidos serão comunicados estão descritos no item 9.5.1 e os documentos pertinentes devem ser revisados.

9.6. Projeto e desenvolvimento de produtos e serviços

A JB3 SOFTWARES S.A. realiza suas atividades de projeto e desenvolvimento de produtos e serviços segundo as etapas documentadas na política POL.004 - Política de Desenvolvimento Seguro.

9.7. Controle de processos, produtos e serviços providos externamente

A JB3 SOFTWARES S.A. realiza suas aquisições mediante a qualificação dos fornecedores e monitoramento periódico da prestação de serviços ou produtos, segundo os procedimentos documentados no processo PRO.007 - Procedimento de Gestão. Seus fornecedores deverão seguir as políticas determinadas pela organização.

9.8. Produção e provisão de serviço

A JB3 SOFTWARES S.A. planeja e realiza a produção e fornecimento de serviço sob condições controladas, como determinado nos procedimentos documentados no SharePoint. Basicamente, a identificação e a rastreabilidade se aplicam a:

- Todos os serviços realizados pela JB3 SOFTWARES S.A. que façam parte do escopo do SGI;
- Todos os serviços de terceiros controlados pela JB3 SOFTWARES S.A. que façam parte do escopo do SGI;

A JB3 SOFTWARES S.A. tem cuidado com a propriedade do cliente enquanto está sob o seu controle ou uso. Conforme apropriado e em acordo com os contratos estabelecidos com os clientes, identifica, verifica, protege e salvaguarda a propriedade do cliente fornecida para uso ou incorporação no produto. Se qualquer propriedade do cliente for perdida, danificada ou considerada inadequada para o uso, isto é informado ao cliente e são mantidos registros, nos sistemas informatizados de suporte ou, quando é necessário tratamento de produto não conforme ou ação corretiva ou preventiva, nos registros estabelecidos pelos correspondentes procedimentos documentados.

9.9. Liberação de Produtos e Serviços

Para garantir a satisfação do cliente, os planejamentos da avaliação de atendimentos dos serviços ficam disponíveis para demonstrar as etapas adequadas, as verificações, responsáveis e critérios de amostragem. A informação para a realização da atividade final só poderá ser liberada ao cliente depois que todas as etapas tenham sido cumpridas e com resultados satisfatórios.
A informação retida contém os resultados obtidos que justifiquem a liberação e a pessoa responsável pela liberação.

9.10. Controle de Saídas Não Conformes

As informações documentadas são retidas, contendo a descrição da não conformidade, as ações tomadas, eventuais concessões obtidas e a autoridade que decidiu as ações em relação à não conformidade.

10. AVALIAÇÃO DE DESEMPENHO

10.1. Monitoramento, Medição, Análise e Avaliação

A organização avalia o desempenho e a eficácia do SGI por meio da análise dos resultados dos indicadores de processos e objetivos, conforme item **7.2. Objetivos de Segurança da Informação e Planejamento para alcançá-los** e dos controles estabelecidos no DOC.006 – Declaração de Aplicabilidade.

10.2. Satisfação do Cliente

A percepção da satisfação do cliente é representada pelo indicador que avalia de forma ampla a satisfação do cliente. Este indicador é a principal referência para melhoria contínua dos produtos e serviços da JB3 SOFTWARES S.A.

10.3. Análise e Avaliação

A organização analisa e avalia dados e informações provenientes do monitoramento e medição dos processos. Os resultados de análises devem ser usados para avaliar: conformidade dos serviços, grau de satisfação do cliente, desempenho e eficácia do SGI, se o planejamento foi implementado eficazmente, a eficácia das ações tomadas para lidar com riscos e oportunidades, desempenho de provedores externos, necessidade de melhorias no SGI.
Os resultados destes processos de análise e avaliação devem ser levados para discussão na Análise Crítica pela Direção.

10.4. Auditoria Interna

A organização conduz anualmente auditorias internas e externas para avaliar a conformidade com as normas ISO e melhores práticas, conforme o planejamento no FOR.005 - Programa de Auditoria e seguindo as diretrizes do PRO.002 - Auditoria Interna

10.5. Análise Crítica Pela Direção

A Alta Direção da organização analisa anualmente e criticamente o SGI para assegurar a sua contínua adequação, pertinência e eficácia. A organização mantém a informação documentada no FOR.002 – Ata de Reunião como evidência dos resultados das análises críticas realizadas pela Alta Direção.

11. MELHORIA

11.1. Melhoria Contínua

A organização melhora continuamente a pertinência, adequação e eficácia do SGI através de planos de melhoria registrados no FOR.007 - Plano de Ação.

11.2. Não Conformidade e Ação Corretiva

Quando uma não conformidade ocorre, a organização cadastra no FOR.007 - Plano de Ação para tratar a causa raiz da não conformidade. As não-conformidades e oportunidade de melhoria são acompanhadas até a solução.

12. HISTÓRICO DE ALTERAÇÕES

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	31/03/2025	Jurídico	Elaboração	Primeira versão
		Diretoria Executiva	Aprovação	
2.0	28/04/2025	Jurídico	Elaboração	Troca do Logo
		Diretoria Executiva	Aprovação	
3.0	15/08/2025	Jurídico	Revisão	Inclusão dos itens pertencentes a 9k e 27018k
		Diretoria Executiva	Aprovação	
4.0	24/09/2025	Jurídico	Revisão	Adequação dos objetivos x processos
		Diretoria Executiva	Aprovação	

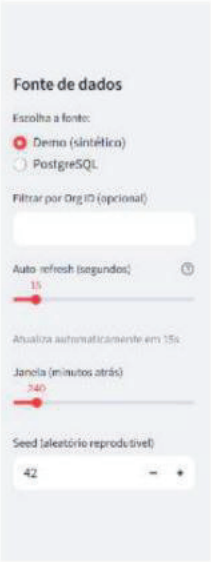
1. Descrição

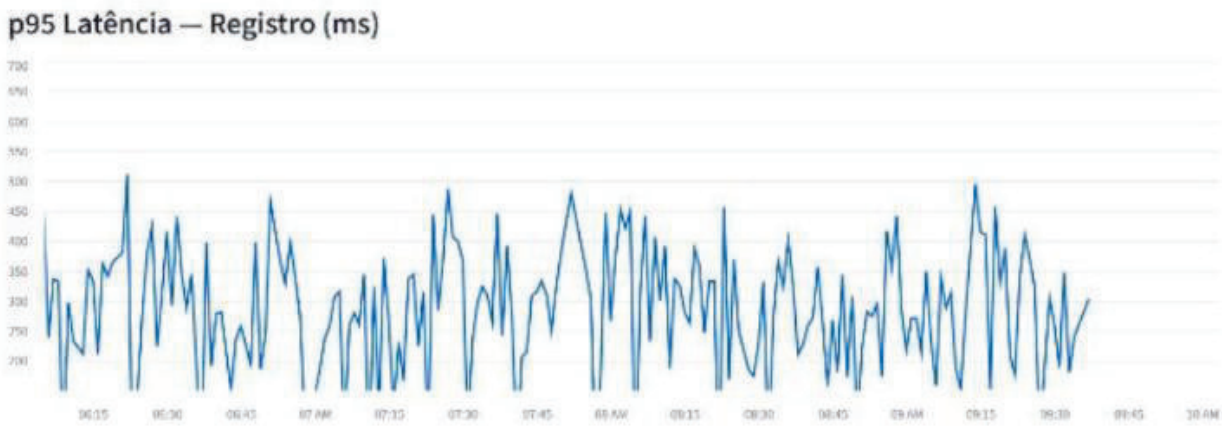
A gerenciadora de consentimentos e ciências possui capacidade de geração de painéis gerenciais e de auditoria, permitindo a visualização consolidada de indicadores, métricas e informações críticas em tempo real. Essa funcionalidade facilita a tomada de decisão estratégica, garante transparência nos processos e oferece recursos para monitoramento e conformidade, reduzindo riscos e aumentando a eficiência operacional.

2. Painéis e relatórios

O painel criado com a ferramenta Grafana serve para monitoramento e visualização de dados em tempo real, sendo utilizado para:
Consolidar informações de diferentes fontes (bancos de dados, APIs, sistemas internos) em um único painel.
Exibir métricas e indicadores-chave por meio de gráficos, tabelas e alertas.
Facilitar a análise gerencial e operacional, permitindo identificar tendências, gargalos ou falhas rapidamente.
Auditar processos e garantir conformidade, com histórico de dados e logs acessíveis.
Configurar alertas automáticos, que notificam quando valores ultrapassam limites definidos.

Link https://grafana.jb3ti.com.br



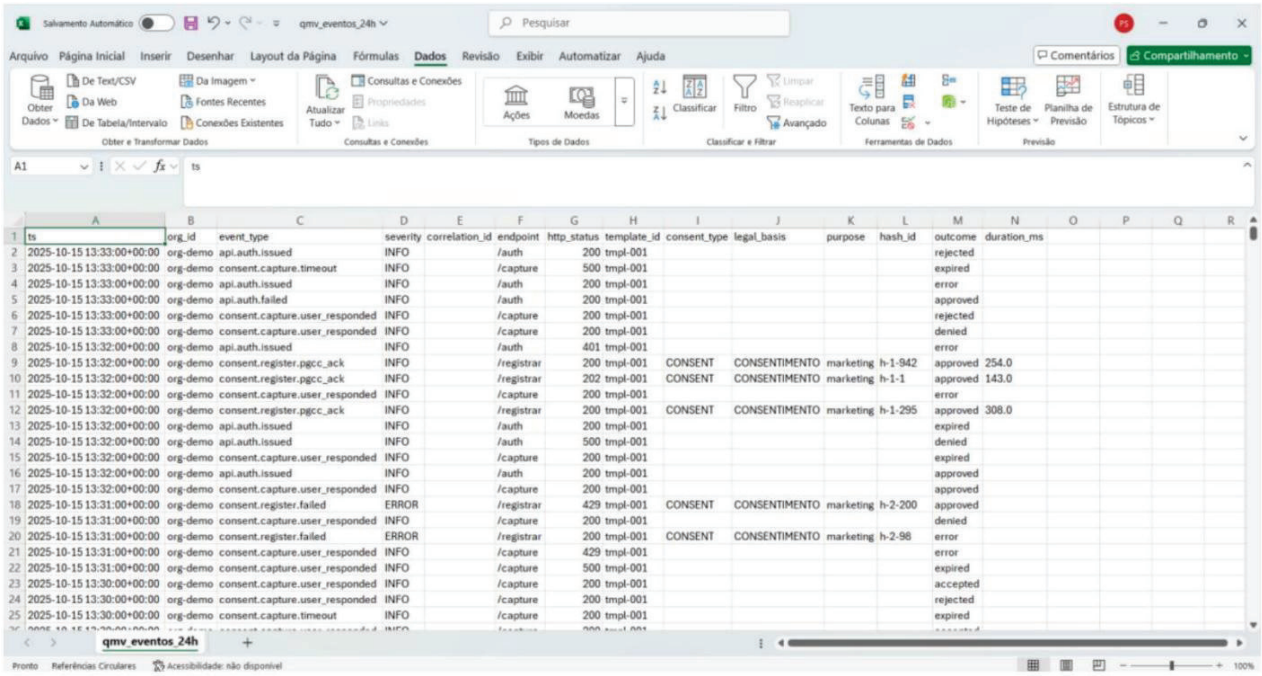


Auditoria — eventos recentes

	ts	org_id	event_type	outcome	http_status	correlation_id	template_id	hash_id	duration_ms
0	2025-10-21 12:38:00+00:00	org-demo	api.auth.issued	rejected	200	None	tmpl-001	None	None
4	2025-10-21 12:38:00+00:00	org-demo	consent.capture.user_responded	rejected	200	None	tmpl-001	None	None
5	2025-10-21 12:38:00+00:00	org-demo	consent.capture.user_responded	denied	200	None	tmpl-001	None	None
1	2025-10-21 12:38:00+00:00	org-demo	consent.capture.timeout	expired	500	None	tmpl-001	None	None
3	2025-10-21 12:38:00+00:00	org-demo	api.auth.failed	approved	200	None	tmpl-001	None	None
2	2025-10-21 12:38:00+00:00	org-demo	api.auth.issued	error	200	None	tmpl-001	None	None
6	2025-10-21 12:37:00+00:00	org-demo	api.auth.issued	error	401	None	tmpl-001	None	None
7	2025-10-21 12:37:00+00:00	org-demo	consent.register.pgcc_ack	approved	200	None	tmpl-001	h-1-942	254
8	2025-10-21 12:37:00+00:00	org-demo	consent.register.pgcc_ack	approved	202	None	tmpl-001	h-1-1	143
9	2025-10-21 12:37:00+00:00	org-demo	consent.capture.user_responded	error	200	None	tmpl-001	None	None

Baixar CSV (eventos 24h)

Possibilita exportar relatórios para acompanhamento dos eventos



ts	org_id	event_type	severity	correlation_id	endpoint	http_status	template_id	consent_type	legal_basis	purpose	hash_id	outcome	duration_ms
2025-10-15 13:33:00+00:00	org-demo	api.auth.issued	INFO		/auth	200	tmpl-001					rejected	
2025-10-15 13:33:00+00:00	org-demo	consent.capture.timeout	INFO		/capture	500	tmpl-001					expired	
2025-10-15 13:33:00+00:00	org-demo	api.auth.issued	INFO		/auth	200	tmpl-001					error	
2025-10-15 13:33:00+00:00	org-demo	api.auth.failed	INFO		/auth	200	tmpl-001					approved	
2025-10-15 13:33:00+00:00	org-demo	consent.capture.user_responded	INFO		/capture	200	tmpl-001					rejected	
2025-10-15 13:33:00+00:00	org-demo	consent.capture.user_responded	INFO		/capture	200	tmpl-001					denied	
2025-10-15 13:32:00+00:00	org-demo	api.auth.issued	INFO		/auth	401	tmpl-001					error	
2025-10-15 13:32:00+00:00	org-demo	consent.register.pgcc_ack	INFO		/registrar	200	tmpl-001	CONSENT	CONSENTIMENTO	marketing	h-1-942	approved	254.0
2025-10-15 13:32:00+00:00	org-demo	consent.register.pgcc_ack	INFO		/registrar	202	tmpl-001	CONSENT	CONSENTIMENTO	marketing	h-1-1	approved	143.0
2025-10-15 13:32:00+00:00	org-demo	consent.capture.user_responded	INFO		/capture	200	tmpl-001					error	
2025-10-15 13:32:00+00:00	org-demo	consent.register.pgcc_ack	INFO		/registrar	200	tmpl-001	CONSENT	CONSENTIMENTO	marketing	h-1-295	approved	308.0
2025-10-15 13:32:00+00:00	org-demo	api.auth.issued	INFO		/auth	200	tmpl-001					expired	
2025-10-15 13:32:00+00:00	org-demo	api.auth.issued	INFO		/auth	500	tmpl-001					denied	
2025-10-15 13:32:00+00:00	org-demo	consent.capture.user_responded	INFO		/capture	200	tmpl-001					expired	
2025-10-15 13:32:00+00:00	org-demo	api.auth.issued	INFO		/auth	200	tmpl-001					approved	
2025-10-15 13:32:00+00:00	org-demo	consent.capture.user_responded	INFO		/capture	200	tmpl-001					approved	
2025-10-15 13:31:00+00:00	org-demo	consent.register.failed	ERROR		/registrar	429	tmpl-001	CONSENT	CONSENTIMENTO	marketing	h-2-200	approved	
2025-10-15 13:31:00+00:00	org-demo	consent.capture.user_responded	INFO		/capture	200	tmpl-001					denied	
2025-10-15 13:31:00+00:00	org-demo	consent.register.failed	ERROR		/registrar	200	tmpl-001	CONSENT	CONSENTIMENTO	marketing	h-2-98	error	
2025-10-15 13:31:00+00:00	org-demo	consent.capture.user_responded	INFO		/capture	429	tmpl-001					error	
2025-10-15 13:31:00+00:00	org-demo	consent.capture.user_responded	INFO		/capture	500	tmpl-001					expired	
2025-10-15 13:30:00+00:00	org-demo	consent.capture.user_responded	INFO		/capture	200	tmpl-001					accepted	
2025-10-15 13:30:00+00:00	org-demo	consent.capture.user_responded	INFO		/capture	200	tmpl-001					rejected	
2025-10-15 13:30:00+00:00	org-demo	consent.capture.timeout	INFO		/capture	200	tmpl-001					expired	

3. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

1. Descrição

A gerenciadora de consentimentos e ciências possui um plano estruturado de segregação de ambientes (TST, HML e PRD), garantindo que cada fase do ciclo de desenvolvimento ocorra em um espaço isolado e seguro.

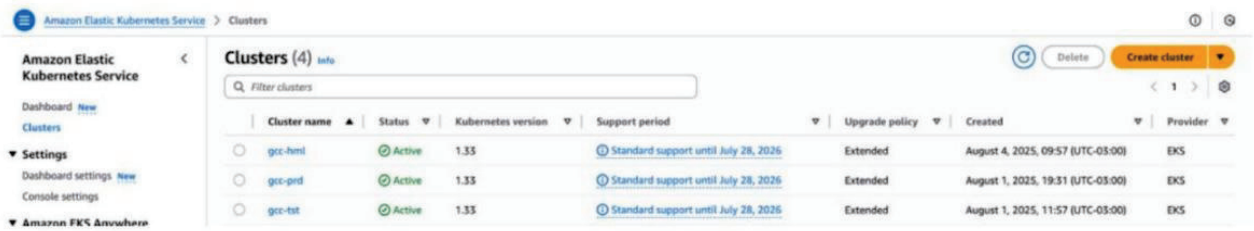
Objetivo: Assegurar qualidade, estabilidade e segurança nas entregas, evitando que testes ou homologações impactem o ambiente produtivo.

Vantagens:
Redução de riscos de falhas em produção.
Maior controle e rastreabilidade das mudanças.
Ambientes dedicados para testes e validações antes da liberação final.
Conformidade com boas práticas de governança e auditoria.

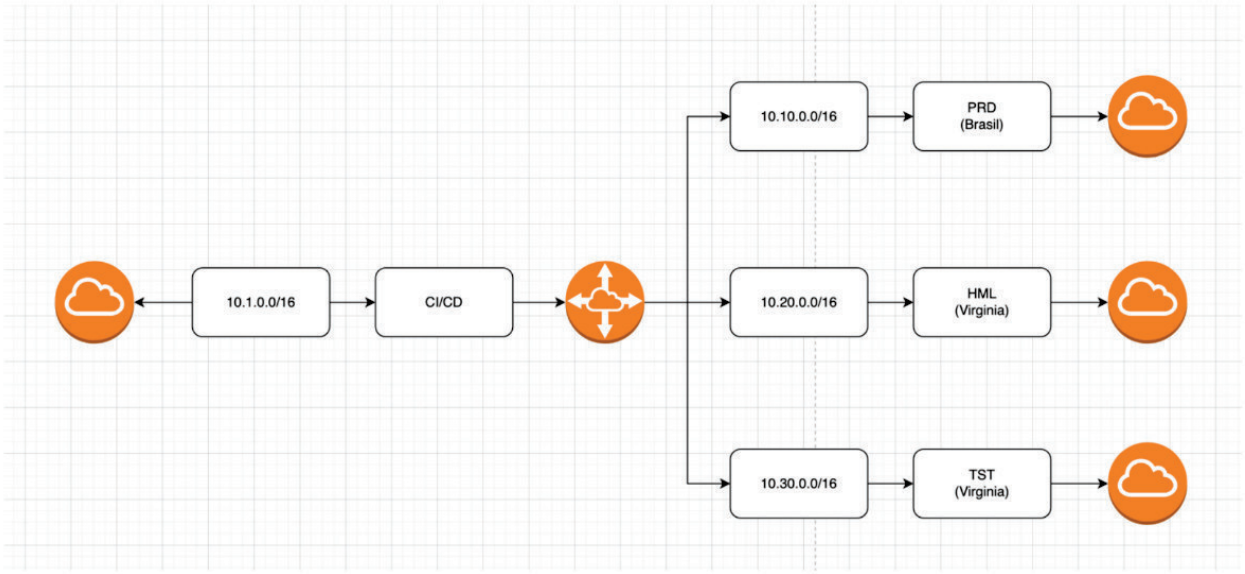
2. Processo automatizado e sistematizado de atualização com controle de versões, rollback e etapas de homologação em ambientes segregados

Possui processo automatizado e sistematizado de atualização com controle de versões, rollback e etapas de homologação em ambientes segregados.

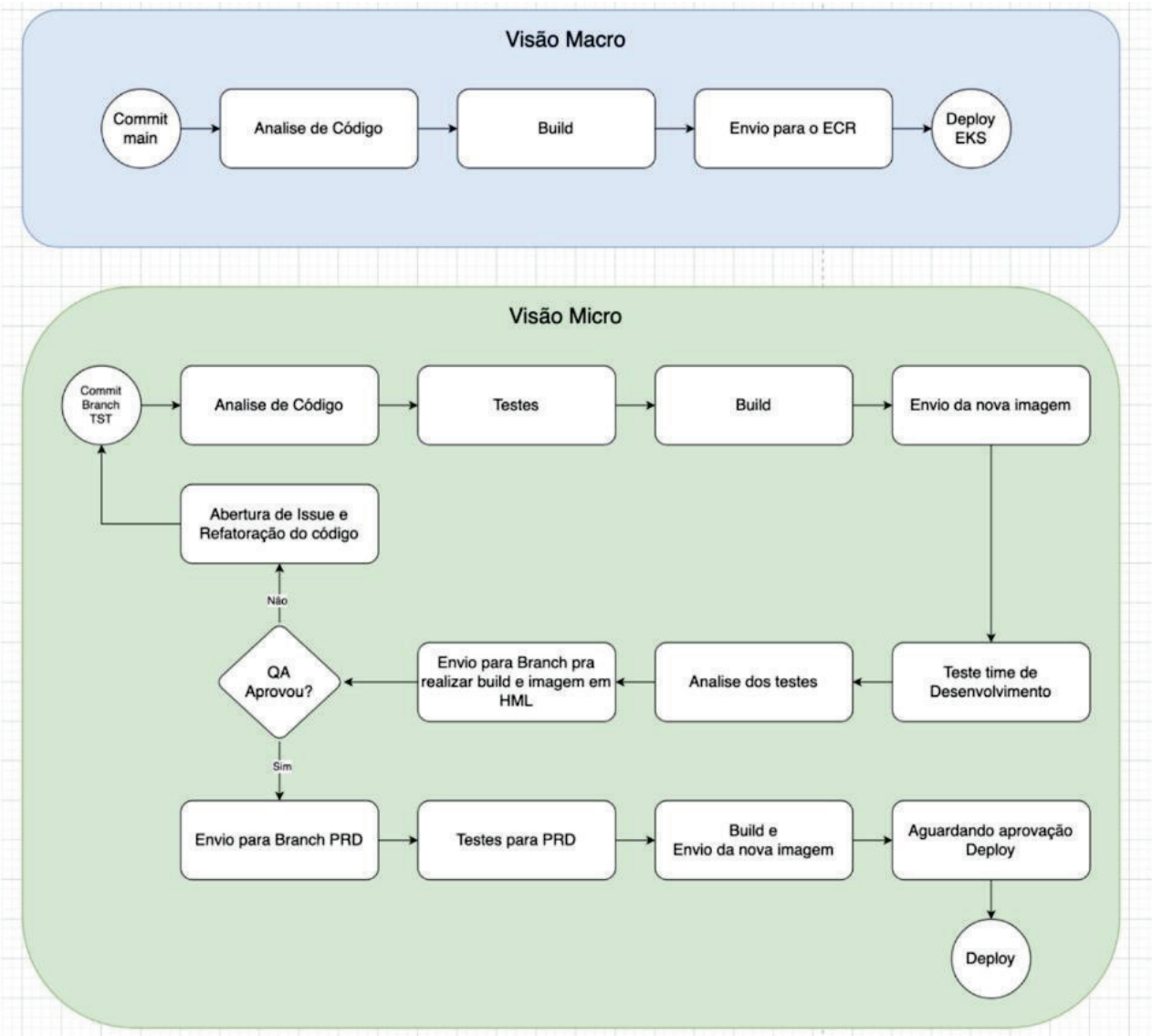
A solução possui implementação de três ambientes completamente segregados:
• Testes
• Homologação
• Produção



A segregação dos 3 ambientes é física. Ambiente de produção encontra-se na AWS Brasil São Paulo, Homologação na AWS USA Virgínia numa VPC e o de testes na AWS USA Virgínia em outra VPC distinta garantindo assim a segregação física e logica de todos ambientes.

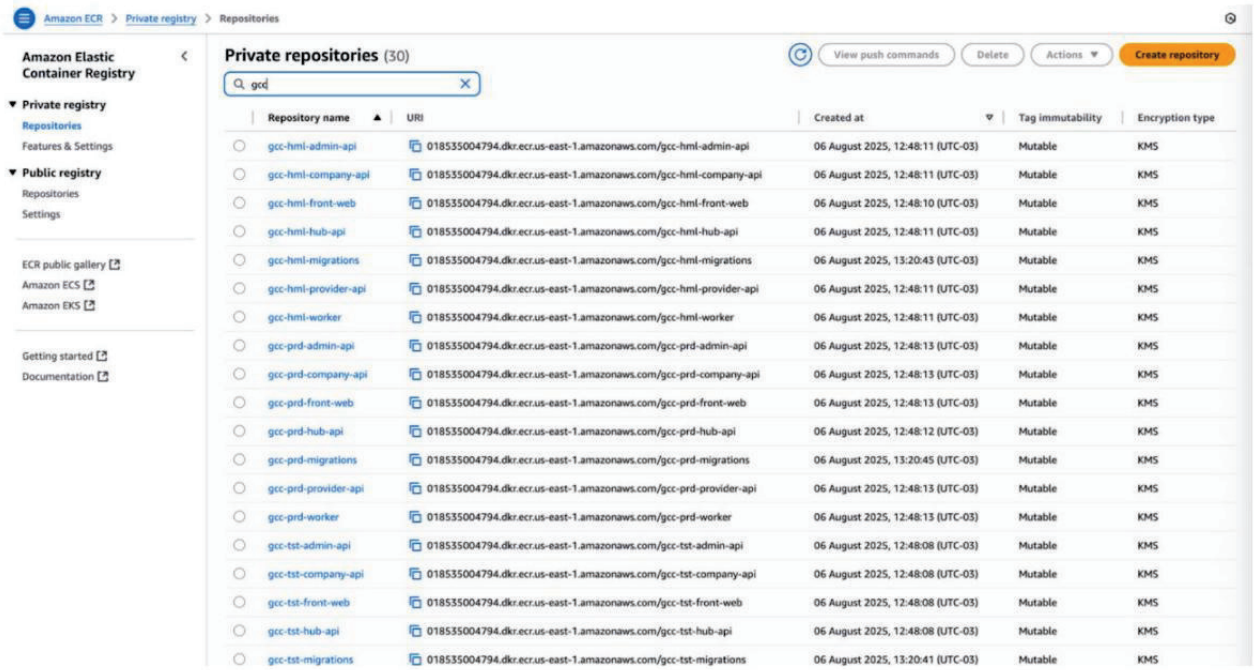


Esta solução garante o fluxo automatizado, com controle de versões para rastreabilidade, capacidade de reverter alterações (rollback) e homologação em ambientes de teste antes da implantação em produção.

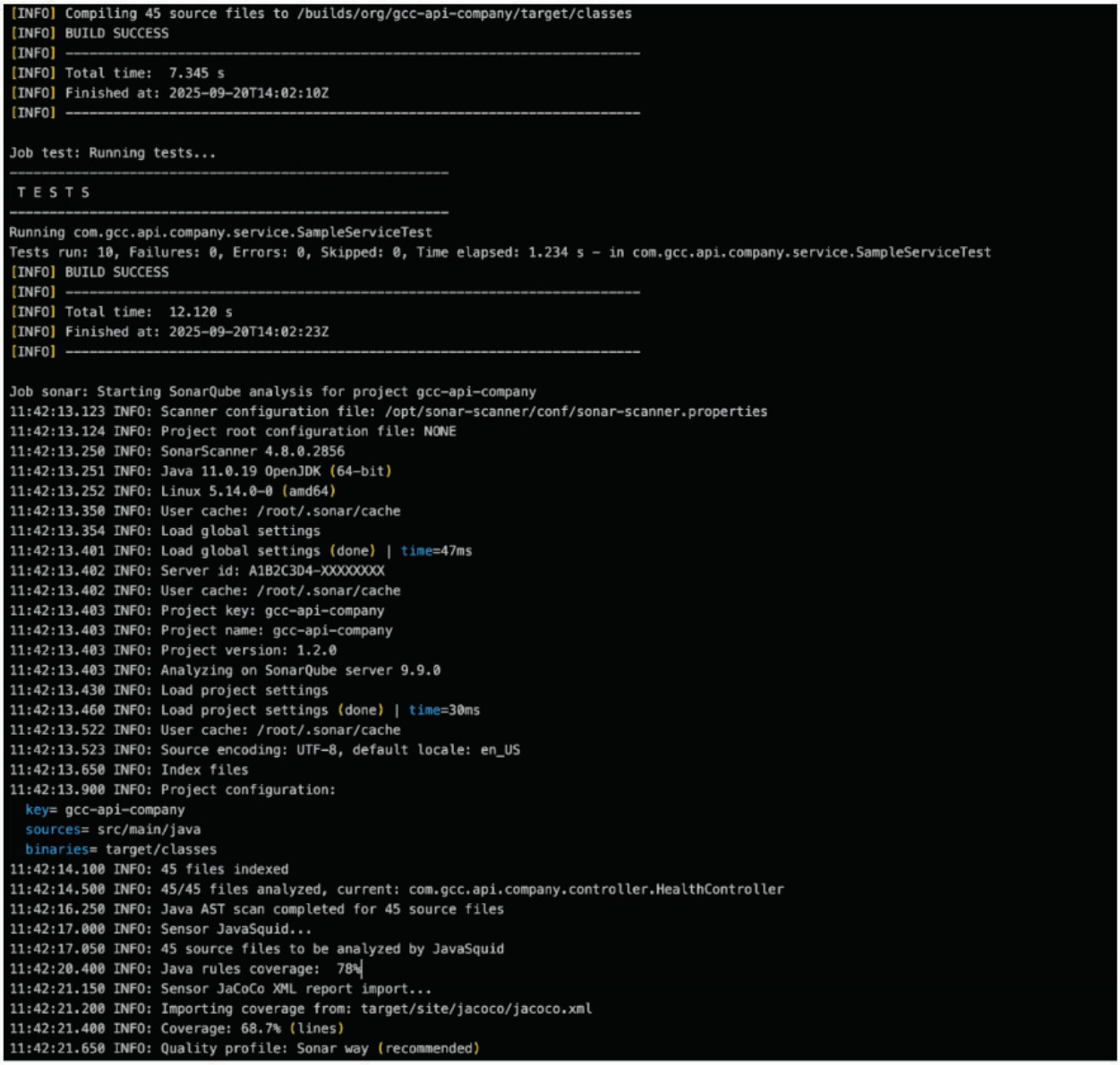


Para esta configuração é usado o GITEA integrado com o Kubernates e outros serviços da AWS, garantindo todo o fluxo automatizado de CI/CD da solução.

Para publicação são criados registos de containers, ficando o respetivo histórico, podendo ser efetuado rollback diretamente pelo CI/CD ou em caso de necessidade extrema via publicação no histórico dos containers. Todos os containers por questões de segurança encontram-se encriptados (KMS).



Para validação de código automatizado são usadas ferramentas com o SonarQube no processo automático de compilação do código.



3. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

Política de Backup

1. Introdução

Esta Política de Backup tem como objetivo estabelecer diretrizes para a criação, armazenamento, recuperação e gerenciamento de cópias de segurança dos dados corporativos da JB3 SOFTWARES S.A., garantindo a continuidade dos negócios e a proteção contra perda de informações.

2. Objetivo

Definir normas para a realização de backups regulares, assegurando a integridade, disponibilidade e recuperação de dados em caso de falhas, incidentes ou desastres.

3. Abrangência

Aplica-se a todos os sistemas, servidores, bancos de dados, dispositivos e informações corporativas, independentemente do local de armazenamento ou do tipo de dado.

4. Diretrizes Gerais

- Backups devem ser realizados regularmente, conforme cronograma definido pela área de TI;
- Dados críticos devem ter backups redundantes armazenados em locais distintos (ex.: armazenamento local e na nuvem);
- Backups devem ser protegidos por criptografia e acessíveis apenas a usuários autorizados;
- Testes de recuperação devem ser realizados periodicamente para garantir a eficácia dos backups.

5. Tipos de Backup

- Backup Completo: Cópia integral de todos os dados, realizada em intervalos definidos;
- Backup Incremental: Cópia apenas dos dados alterados desde o último backup;
- Backup Diferencial: Cópia dos dados alterados desde o último backup completo;
- Backup em Nuvem: Armazenamento de dados em provedores de nuvem confiáveis, garantindo redundância e escalabilidade.

6. Requisitos de Armazenamento

- Backups devem ser armazenados em locais seguros, protegidos contra acesso não autorizado, danos físicos ou cibernéticos;
- É obrigatório o uso de criptografia para proteger dados sensíveis armazenados em backups;
- Backups e logs de auditoria deverão ser mantidos por um período mínimo de 05 (cinco) anos, salvo disposição legal específica que determine prazo superior;
- Backups devem ser mantidos por períodos definidos, conforme regulamentações legais e políticas internas.

7. Responsabilidades

- Área de TI: Planejar, executar e monitorar backups, além de realizar testes de recuperação;
- Compliance: Garantir que a política esteja alinhada às regulamentações aplicáveis;
- Colaboradores: Seguir as diretrizes estabelecidas e reportar incidentes relacionados à perda de dados.

8. Recuperação de Dados

- Procedimentos de recuperação devem ser documentados e testados regularmente;
- A recuperação de dados deve ser realizada apenas por pessoal autorizado;
- Incidentes que exijam recuperação de dados devem ser reportados e analisados para evitar recorrências.

9. Monitoramento e Revisão

- A política será revisada anualmente ou sempre que houver alterações legais ou tecnológicas relevantes;
- Auditorias internas serão realizadas para garantir a conformidade com esta política.

10. Base Legal

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD);
- Normas ISO 27001 (Gestão de Segurança da Informação) e ISO 22301 (Gestão de Continuidade de Negócios).

11. DISPOSIÇÕES FINAIS

O descumprimento desta política poderá resultar em medidas disciplinares, conforme previsto nos regulamentos internos.

12. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política de Backup	Manual de Procedimentos	31/03/2025	1.0

Data	Descrição Ação	Versão	Responsável
31/03/2025	Elaboração	1.0	Jurídico
31/03/2025	Revisado e Aprovado	2.0	Diretoria Executiva

Política de Criptografia

1. Introdução

Esta Política de Criptografia tem como objetivo estabelecer diretrizes para o uso de criptografia na proteção de dados sensíveis e informações corporativas da JB3 SOFTWARES S.A., garantindo a segurança, confidencialidade e integridade dos dados.

2. Objetivo

Definir normas para a aplicação de criptografia em sistemas, dispositivos e processos, prevenindo acessos não autorizados e garantindo a conformidade com legislações e regulamentações aplicáveis.

3. Abrangência

Aplica-se a todos os colaboradores, prestadores de serviços, parceiros e fornecedores que lidem com dados sensíveis ou informações corporativas, independentemente do meio ou dispositivo utilizado.

4. Diretrizes Gerais

- Dados sensíveis devem ser protegidos por criptografia em repouso (armazenamento) e em trânsito (transferência);
- Apenas algoritmos de criptografia reconhecidos como seguros devem ser utilizados (ex.: AES, RSA, SHA-256);
- Chaves de criptografia devem ser gerenciadas de forma segura e acessíveis apenas a usuários autorizados;
- A criptografia deve ser aplicada em conformidade com a Lei Geral de Proteção de Dados (LGPD) e outras regulamentações aplicáveis.

5. Requisitos de Criptografia

- Dados em repouso: Informações armazenadas em servidores, bancos de dados e dispositivos devem ser protegidas por criptografia de disco ou arquivo;
- Dados em trânsito: Informações transmitidas por redes internas ou externas devem ser protegidas por protocolos seguros, como TLS ou VPN;

- Gestão de chaves: Chaves de criptografia devem ser geradas, armazenadas e descartadas de forma segura, utilizando ferramentas de gerenciamento de chaves;

- Autenticação: O acesso a dados criptografados deve ser restrito a usuários autorizados, mediante autenticação robusta (ex.: autenticação multifator).

6. Responsabilidades

- Área de TI: Implementar e monitorar soluções de criptografia, gerenciar chaves e realizar auditorias periódicas;

- Compliance: Garantir que a política esteja alinhada às regulamentações aplicáveis;

- Colaboradores: Seguir as diretrizes estabelecidas e reportar incidentes relacionados à segurança de dados.

7. Restrições

- É proibido o uso de algoritmos de criptografia obsoletos ou vulneráveis (ex.: MD5, DES);

- Dados sensíveis não devem ser armazenados ou transmitidos sem criptografia adequada;

- Chaves de criptografia não devem ser compartilhadas ou armazenadas em locais inseguros.

8. Monitoramento e Revisão

- A política será revisada anualmente ou sempre que houver alterações legais ou tecnológicas relevantes;

- Auditorias internas e testes de segurança serão realizados para garantir a conformidade com esta política.

9. Base Legal

- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD);

- Normas ISO 27001 (Gestão de Segurança da Informação) e ISO 27701 (Privacidade da Informação).

10 DISPOSIÇÕES FINAIS

O descumprimento desta política poderá resultar em medidas disciplinares, conforme previsto nos regulamentos internos da JB3 SOFTWARES S.A.

11. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política Criptografia	Manual de Procedimentos	31/03/2025	1.0

Data	Descrição Ação	Versão	Responsável
31/03/2025	Elaboração	1.0	Jurídico
31/03/2025	Revisado e Aprovado	2.0	Diretoria Executiva

Política de Gestão da Continuidade do Negócio

1. Introdução

A resiliência empresarial em face de adversidades e interrupções imprevistas é um aspecto crucial para a sustentabilidade e o sucesso de longo prazo de qualquer organização. Neste contexto, o Plano de Gestão da Continuidade do Negócio é uma ferramenta essencial que estabelece uma abordagem sistêmica e estratégica para assegurar a continuidade das operações críticas sob quaisquer circunstâncias. Este documento delineia não apenas as diretrizes e responsabilidades das equipes envolvidas nas operações de continuidade, mas também engloba procedimentos detalhados para resposta a incidentes, gestão de crises, e recuperação efetiva após desastres.

A política incorpora uma análise aprofundada dos impactos potenciais sobre o negócio, identificando os ativos críticos, especialmente aqueles dependentes de sistemas de TI, e avaliando os riscos associados a diferentes cenários de interrupção. Além disso, contempla estratégias de adaptação e mudanças no planejamento para enfrentar desafios emergentes, assegurando a agilidade e flexibilidade do negócio. Informações vitais, como a Análise de Impacto nos Negócios, listas de contato essenciais, e considerações sobre implicações financeiras, são meticulosamente detalhadas e anexadas para oferecer um panorama abrangente e um roteiro claro para a continuidade operacional.

A eficácia deste plano está intrinsecamente ligada ao seu caráter dinâmico e adaptativo, com revisões e atualizações regulares para refletir o ambiente de negócios em constante mudança, bem como os avanços tecnológicos. A implementação deste plano é fundamental para minimizar interrupções, proteger os interesses dos stakeholders, e garantir a sustentabilidade e resiliência da organização no longo prazo.

2. Propósito

Análise de Impacto nos Negócios (BIA): Este é um processo crítico que envolve uma avaliação detalhada dos efeitos de uma interrupção nos processos de negócios. Na JB3 SOFTWARES S.A., a BIA deve ir além da identificação dos processos críticos, englobando também a determinação do impacto financeiro, operacional e de reputação, e a identificação do tempo máximo tolerável de interrupção para cada processo.

Gestão de Continuidade de Negócios (GCN): A GCN na JB3 SOFTWARES S.A. é um processo holístico de gestão, visando não apenas a resiliência organizacional, mas também a agilidade e flexibilidade para responder a eventos inesperados. É fundamental que a GCN inclua estratégias para lidar com uma ampla gama de cenários de interrupção, desde desastres naturais até ciberataques.

Gestor de Negócio: O papel do gestor de negócio é crucial, pois ele deve não só gerenciar os processos críticos, mas também participar ativamente na elaboração e implementação de estratégias de continuidade e recuperação. É importante que esses gestores tenham um entendimento claro dos objetivos estratégicos da companhia e como os processos sob sua responsabilidade se alinham a esses objetivos.

Objetivos de Recuperação: Definir objetivos de recuperação claros e realistas é vital. Estes devem ser baseados em uma compreensão do impacto operacional, financeiro e de reputação de uma interrupção. É importante que estes objetivos sejam regularmente revistos e ajustados conforme as mudanças nos processos de negócios e no ambiente operacional.

Planos de Continuidade de Negócios: Os planos de continuidade devem ser documentos vivos, regularmente testados e atualizados. Eles devem detalhar não apenas as ações de recuperação, mas também estratégias proativas para mitigação de riscos. A comunicação durante uma crise é crucial e deve ser gerenciada de forma a manter todas as partes interessadas informadas e engajadas.

Sistema de Gestão de Continuidade de Negócios (SGCN): O SGCN deve ser uma estrutura de governança integrada, apoiada pelo comprometimento da alta direção. Este sistema deve ser abrangente, cobrindo desde a identificação de riscos até a implementação e manutenção de estratégias e planos de recuperação. A eficácia do SGCN depende do compromisso contínuo com a melhoria e adaptação às mudanças no ambiente de negócios e tecnológico.

3. Diretrizes

O sistema de gestão de continuidade do negócio da companhia deve prever mecanismos que permitam:

Identificar ameaças internas e externas, é fundamental realizar uma análise detalhada e contínua dessas ameaças, considerando as tendências do mercado e as mudanças no ambiente operacional. Ferramentas como análise SWOT (Strengths, Weaknesses, Opportunities, Threats) e PESTEL (Political, Economic, Social, Technological, Environmental, Legal) podem ser úteis nesse processo.

Avaliar os possíveis impactos não deve se limitar apenas aos efeitos imediatos, mas também considerar as consequências a longo prazo nas operações da Companhia. Essa análise deve incluir cenários variados, desde desastres naturais até falhas tecnológicas e ciberataques.

A identificação de requisitos para a continuidade dos negócios deve ser um processo abrangente, que considere não apenas aspectos legais e regulatórios, mas também fatores como sustentabilidade operacional, reputação da empresa e expectativas dos stakeholders.

A definição clara de papéis e responsabilidades deve se estender a todas as partes envolvidas, incluindo fornecedores e parceiros externos. É importante estabelecer canais de comunicação eficazes e planos de ação específicos para cada grupo.

A estrutura de gerenciamento de crises deve ser robusta, com planos de comunicação claros, incluindo protocolos para comunicação interna e externa. Além disso, é vital ter um plano de sucessão de liderança para garantir a continuidade da tomada de decisões em situações de crise.

Os processos de recuperação devem ser realistas e testados regularmente. Eles devem incluir procedimentos detalhados para a restauração de operações críticas, incluindo sistemas de TI, infraestrutura e recursos humanos.

Os testes dos planos de continuidade devem ser frequentes e abrangentes, incluindo simulações de cenários variados para avaliar a eficácia e a prontidão das equipes. As análises devem levar em consideração os feedbacks desses testes e promover a melhoria contínua dos planos.

4. Definições e tempo de recuperação

Tempo de Recuperação Objetivo (RTO - *Recovery Time Objective*)

O RTO determina o tempo máximo aceitável para restaurar os serviços após uma falha ou desastre. Considerando a infraestrutura de alta disponibilidade e os requisitos de continuidade, os tempos de recuperação são definidos conforme a criticidade dos sistemas:

Tipo de Sistema	Descrição	RTO Definido
Sistemas Críticos	Aplicações essenciais ao negócio, como transações financeiras e plataformas operacionais.	Até 1 hora
Sistemas Essenciais	Sistemas administrativos, gestão de clientes, CRM.	Até 4 horas
Sistemas de Suporte	Documentos, backups, dados históricos.	Até 24 horas

A recuperação para sistemas críticos deve ser prioritária para garantir a continuidade das operações sem impactos aos clientes.

Ponto de Recuperação Objetivo (RPO - *Recovery Point Objective*)

O RPO define a quantidade máxima de dados que pode ser perdida em caso de falha sem afetar criticamente o negócio. Considerando a política de backups e recuperação de desastres, os tempos estabelecidos são:

Tipo de Sistema	Descrição	RPO Definido
Sistemas Críticos	Base de dados transacionais, serviços online, processamento OCR.	Até 15 minutos
Sistemas Essenciais	Informações administrativas, relatórios financeiros.	Até 4 horas
Sistemas de Suporte	Documentos estáticos, arquivos não essenciais.	Até 12 horas

Para sistemas críticos, a estratégia recomendada é a replicação contínua de dados para evitar perda de informações relevantes.

Tempo Máximo Tolerável de Interrupção (MTPD - *Maximum Tolerable Period of Disruption*)

O MTPD define o tempo máximo que um serviço pode ficar indisponível antes de causar impactos irreversíveis ao negócio.

Tipo de Sistema	Descrição	MTPD Definido
Sistemas Críticos	Aplicações operacionais vitais para clientes.	Até 2 horas
Sistemas Essenciais	Sistemas administrativos e de gestão interna.	Até 6 horas
Sistemas de Suporte	Arquivos históricos e documentos de referência.	Até 48 horas

O MTPD deve ser inferior ao RTO, garantindo que a recuperação seja iniciada antes que os impactos sejam severos para a empresa e seus clientes.

1. **Responsáveis**
    - Diretoria
    - Responsável por Segurança da Informação

2. **Disponibilidade do Negócio**

Em relação a infraestrutura e sistemas, haverá necessidade de seguir as definições abaixo pensando no contexto a gestão de continuidade com alta disponibilidade para manter o negócio sem impactos aos clientes.

Infraestrutura Física Robusta: O data center deve ser construído com infraestrutura física resistente a desastres naturais e ataques físicos. Isso inclui a construção em zonas com baixo risco de desastres naturais, estruturas reforçadas, e sistemas de segurança física avançados.

Redundância de Dados e Sistemas: A redundância é vital para a continuidade dos negócios. Isso significa ter múltiplas cópias de dados críticos armazenados em locais diferentes e sistemas de failover automático para garantir que, em caso de falha em um local, outro possa assumir imediatamente.

Proteção contra Ataques Cibernéticos: Em tempos de guerra e crise, os ataques cibernéticos tendem a aumentar. Portanto, é essencial ter uma proteção robusta contra esses ataques, incluindo firewalls avançados, sistemas de detecção e prevenção de intrusos, e constantes auditorias de segurança.

Planos de Recuperação de Desastres (DRP): Um plano de recuperação de desastres bem elaborado deve estar em vigor. Este plano deve incluir procedimentos detalhados para a recuperação rápida de operações de TI após qualquer interrupção, seja devido a desastres naturais, falhas técnicas ou ataques cibernéticos.

Backup e Recuperação: Implementar rotinas de backup consistentes e testadas, com armazenamento tanto on-site quanto off-site. Isso assegura que, mesmo em casos extremos de perda de dados, seja possível recuperá-los eficientemente.

Testes de Continuidade de Negócios: Realizar testes regulares de continuidade de negócios para garantir que todos os sistemas, procedimentos e equipamentos funcionem conforme o esperado em cenários de crise.

Gerenciamento de Crise e Comunicação: Ter uma equipe dedicada para gerenciamento de crise, capaz de tomar decisões rápidas e eficientes. Além disso, manter canais de comunicação claros com clientes, fornecedores e autoridades é crucial durante crises.

Parcerias Estratégicas: Estabelecer parcerias com fornecedores de serviços e outras entidades que possam oferecer suporte adicional em tempos de crise.

Compliance e Regulamentações: Garantir a conformidade com as leis e regulamentações locais e internacionais relevantes, especialmente aquelas relacionadas à proteção de dados e privacidade.

3. Plano de Testes

Esta política define a realização de testes de ambiente de forma semestral. O plano de teste contempla todos os passos e etapas obrigatórios para conformidade dos ambientes.

O plano está definido no documento Plano de Testes e Resultado - Gestão de Continuidade de Ambientes_v1_17052024.

4. Alteração da Política

Esta política pode ser revisada e atualizada pelo CGSIP, sujeita à aprovação final da Direção Executiva.

5. Disposições Finais

Esta política entra em vigor na data de sua aprovação e é vinculativa para todos os membros da organização.

6. Gestão da Política

A responsabilidade pela gestão desta política é atribuída à equipe de segurança da informação, que será responsável por manter, revisar e atualizar conforme necessário.

7. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política de Gestão da Continuidade do Negócio	Manual de Procedimentos	31/01/2025	1.0

Data	Descrição Ação	Versão	Responsável
31/04/2025	Elaboração	1.0	Jurídico
31/04/2025	Revisado e Aprovado	2.0	Diretoria Executiva

Política de Gestão de Incidentes de Segurança da Informação

1. Introdução

Esta política estabelece diretrizes para a gestão eficaz de incidentes de segurança da informação na JB3 SOFTWARES S.A. Ela serve como um complemento ao documento anexo e destina-se a garantir uma resposta rápida e eficiente a incidentes que possam afetar a integridade, confidencialidade e disponibilidade dos ativos de informação da empresa.

2. Propósito

O propósito desta política é fornecer um framework padronizado para a identificação, notificação, resposta e resolução de incidentes de segurança da informação, minimizando o impacto adverso nas operações da empresa e reduzindo o risco de danos.

3. Escopo

Esta política aplica-se a todos os funcionários, contratados, consultores, parceiros e qualquer outra pessoa que tenha acesso aos recursos de informação da JB3 SOFTWARES S.A.

Todos os incidentes de segurança, independentemente da sua natureza, devem ser tratados com seriedade e de acordo com os procedimentos estabelecidos nesta política.

Esta política é aplicável a todas as formas de dados e sistemas de informação utilizados pela JB3 SOFTWARES S.A., incluindo, mas não se limitando a dados eletrônicos e físicos, redes de computadores, sistemas de comunicação e dispositivos portáteis.

4. Conceito

Um incidente de segurança da informação é qualquer evento que possa comprometer a segurança dos ativos de informação da JB3 SOFTWARES S.A., incluindo violações de dados, ataques cibernéticos, perda de dados, ou falhas de segurança.

5. Diretrizes

- Notificação de Incidentes: Qualquer suspeita ou ocorrência de incidente deve ser imediatamente notificada à Diretoria e aos Responsáveis pela Segurança da Informação:
  - através do e-mail
  - através do portal http://www.jb3ti.com.br caso o cliente tenha cadastro efetuado

- Avaliação e Resposta: A equipe de segurança da informação deve avaliar rapidamente o incidente e tomar as medidas necessárias para mitigar os danos e prevenir futuras ocorrências.

- Registro e Documentação: Todos os incidentes devem ser registrados e documentados para análise futura e melhoria contínua dos processos de segurança.

6. Sanções e Conformidade

O descumprimento desta política pode resultar em sanções disciplinares, incluindo, mas não se limitando a, advertência, suspensão ou até mesmo demissão, dependendo da gravidade do incidente.

7. Revisões

Serão realizadas auditorias regulares para garantir a conformidade com esta política. O monitoramento contínuo será implementado para identificar e responder rapidamente a possíveis incidentes de segurança.

Esta política deve ser revisada anualmente ou sempre que houver mudanças significativas nas tecnologias ou processos da empresa, para garantir sua eficácia e relevância.

8. Validade

Esta política entra em vigor a partir da data de sua aprovação e permanece válida até nova revisão.

9. Gestão da Política

A Diretoria e os Responsáveis pela Segurança da Informação são os encarregados pela gestão desta política, garantindo sua implementação, cumprimento e revisão periódica.

10. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política de Gestão de Incidentes	Manual de Procedimentos	31/03/2025	1.0

Data	Descrição Ação	Versão	Responsável
31/03/2025	Elaboração	1.0	Jurídico
	Revisado e Aprovado	2.0	Diretoria Executiva

POLÍTICA DE GESTÃO DE RESÍDUOS ELETRÔNICOS

1. Introdução

Estabelecer diretrizes para o gerenciamento correto, seguro e ambientalmente responsável dos resíduos eletrônicos gerados pelas atividades desta empresa, visando a minimização dos impactos ambientais e o cumprimento das normas legais vigentes.

2. Abrangência

Esta política se aplica a todos os colaboradores, prestadores de serviço, fornecedores e parceiros que utilizam, manuseiam ou descartam equipamentos eletrônicos e seus componentes.

3. Definições

Resíduo Eletrônico: Equipamentos eletrônicos ou componentes que foram descartados, incluindo, mas não se limitando a computadores, monitores, celulares, baterias, impressoras, cabos, entre outros.

Destinação Final: Procedimento de descarte, reutilização, reciclagem ou tratamento dos resíduos eletrônicos, conforme normas ambientais.

4. Diretrizes

4.1. Redução e Reutilização

Priorizar a redução do uso de equipamentos eletrônicos descartáveis.

Incentivar a reutilização de equipamentos em bom estado, quando possível.

4.2. Coleta e Armazenamento

Os resíduos eletrônicos devem ser coletados de forma segregada em pontos específicos designados pela empresa.

O armazenamento deve garantir a segurança, evitar danos ambientais e proteger dados armazenados.

4.3. Descarte e Destinação Final

Os resíduos eletrônicos serão encaminhados exclusivamente para empresas certificadas e autorizadas para reciclagem e tratamento ambientalmente correto.

É proibido o descarte de resíduos eletrônicos em lixo comum, vias públicas ou locais inadequados.

4.4. Conscientização e Capacitação

Promover treinamentos e campanhas de conscientização para colaboradores sobre a importância da gestão adequada dos resíduos eletrônicos.

4.5. Conformidade Legal

Cumprir todas as normas e regulamentações ambientais federais, estaduais e municipais relacionadas à gestão de resíduos eletrônicos, como a Política Nacional de Resíduos Sólidos (Lei nº 12.305/2010).

5. Responsabilidades

Colaboradores: Seguir as orientações da política, descartando resíduos eletrônicos nos locais indicados.

Gestão Ambiental / Equipe Responsável: Coordenar a coleta, armazenamento, destinação e controle dos resíduos eletrônicos.

Fornecedor de Reciclagem: Apresentar comprovação de destinação correta e dar retorno para a empresa.

6. Monitoramento e Revisão

Esta política será revisada anualmente ou sempre que houver mudanças legais ou operacionais significativas.

Relatórios periódicos sobre a gestão dos resíduos eletrônicos serão elaborados para análise e melhorias contínuas.

7. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política de Gestão de Resíduos Eletrônicos	Manual de Procedimentos	30/04/2025	1.0

Data	Descrição Ação	Versão	Responsável
30/04/2025	Elaboração	1.0	Jurídico
30/04/2025	Revisado e Aprovado	2.0	Diretoria Executiva

POLÍTICA DE INCLUSÃO SOCIAL

1. Introdução

Estabelecer diretrizes e compromissos para promover a inclusão social, a diversidade e a igualdade de oportunidades, fomentando um ambiente de trabalho respeitoso, justo e acolhedor para todos.

2. Abrangência

Aplica-se a todos os colaboradores, gestores, fornecedores, parceiros e demais terceiros que atuam em nome ou benefício da JB3 SOFTWARES S.A.

3. Princípios Fundamentais

Diversidade: Valorizar e respeitar as diferenças de gênero, raça, etnia, orientação sexual, idade, deficiência, religião, origem socioeconômica e outras condições pessoais.

Igualdade de Oportunidades: Garantir processos justos e equitativos de recrutamento, seleção, desenvolvimento e promoção.

Combate à Discriminação: Prevenir e combater todas as formas de discriminação, assédio, preconceito e exclusão.

Acessibilidade: Promover condições adequadas para a inclusão plena de pessoas com deficiência.

Ambiente Respeitoso: Fomentar um ambiente de trabalho seguro, saudável e respeitador, onde todos se sintam valorizados e incluídos.

4. Diretrizes

4.1. Cumprir integralmente a legislação vigente relacionada a direitos humanos, trabalho e inclusão, incluindo a Lei nº 13.146/2015 (Estatuto da Pessoa com Deficiência) e normas correlatas.

4.2. Implementar práticas de recrutamento e seleção que promovam a diversidade e a inclusão, buscando eliminar vieses e barreiras.

4.3. Desenvolver programas de capacitação e sensibilização para gestores e colaboradores sobre diversidade, inclusão e combate ao preconceito.

4.4. Estimular a participação de grupos sub-representados em todos os níveis hierárquicos da empresa.

4.5. Assegurar adaptações e condições de trabalho adequadas para pessoas com deficiência e demais necessidades específicas.

4.6. Manter canais de comunicação abertos para o relato de condutas discriminatórias, garantindo confidencialidade e proteção contra retaliação.

4.7. Promover ações e parcerias com a comunidade para fomentar a inclusão social e o desenvolvimento sustentável.

5. Compromisso da Alta Administração

A alta administração desta empresa se compromete a:

Liderar pelo exemplo, promovendo uma cultura inclusiva;

Disponibilizar recursos para implementar e fortalecer as ações de inclusão;

Garantir o monitoramento e avaliação periódica das práticas de diversidade e inclusão.

6. Responsabilidades

Colaboradores: Respeitar as diferenças e contribuir para um ambiente inclusivo e acolhedor.

Gestores: Promover e garantir a aplicação desta política nas suas equipes.

Área de Recursos Humanos e Compliance: Coordenar ações, monitorar indicadores e assegurar o cumprimento da política.

7. Comunicação e Transparência

Esta empresa se compromete-se a divulgar de forma transparente as ações, avanços e desafios relacionados à inclusão social, estimulando o diálogo e a participação de todos.

8. Revisão a Atualização

Esta política será revisada periodicamente para assegurar sua atualização e conformidade com as melhores práticas e a legislação vigente.

9. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política de Inclusão Social	Manual de Procedimentos	30/04/2025	1.0

Data	Descrição Ação	Versão	Responsável
30/04/2025	Elaboração	1.0	Jurídico
30/04/2025	Revisado e Aprovado	2.0	Diretoria Executiva

POLÍTICA DE INTEGRIDADE

1. Introdução

Estabelece diretrizes e compromissos que garantem a conduta ética, a conformidade legal e o combate a práticas ilícitas em todas as atividades da JB3 SOFTWARES S.A., promovendo uma cultura sólida de integridade, transparência e responsabilidade corporativa.

2. Abrangência

Aplica-se a todos os colaboradores, dirigentes, prestadores de serviços, fornecedores, parceiros comerciais e demais terceiros que mantenham relações com a JB3 SOFTWARES S.A.

3. Princípios Fundamentais

Ética e Transparência;

Compromisso com a Lei;

Responsabilidade Corporativa;

Prevenção e Combate à Corrupção;

Respeito aos Direitos Humanos e à Diversidade;

Proteção e Segurança da Informação;

Cultura de Denúncia e Proteção ao Denunciante.

4. Diretrizes

4.1. Esta empresa implementa, mantém e exige o cumprimento das seguintes políticas integradas que formam seu Programa de Integridade:

Código de Conduta;

Política Antissuborno e Anticorrupção;

Política de Conflito de Interesses;

Política de Segurança da Informação;

Outras políticas complementares aplicáveis.

4.2. A alta administração desta empresa compromete-se a:

Fornecer recursos e liderança para a implementação eficaz do Programa de Integridade;

Garantir independência e autonomia das áreas de Compliance e Jurídico;

Revisar periodicamente os programas e políticas para aprimoramento contínuo.

4.3. Todos os colaboradores e terceiros devem:

Conhecer, entender e cumprir integralmente as políticas de integridade;

Participar dos treinamentos e capacitações;

Utilizar os canais oficiais para reportar dúvidas, irregularidades e suspeitas de violações;

Cooperar com as investigações internas e auditorias.

5. Comunicação e Treinamento

Esta empresa promove treinamentos periódicos para disseminar a cultura de integridade e reforçar o compromisso com as políticas internas e a legislação vigente.

6. Monitoramento e Auditoria

O Programa de Integridade é submetido a monitoramento contínuo e auditorias internas, baseados em matriz de riscos, para assegurar sua eficácia e adequação.

7. Canal de Denúncias e Proteção ao Denunciante

A JB3 SOFTWARES S.A. mantém um canal de denúncias acessível 24 horas, garantindo o sigilo, o anonimato e a proteção contra qualquer forma de retaliação a quem reportar de boa-fé.

8. Sanções

O descumprimento das políticas de integridade, legislação aplicável e normas internas sujeita os infratores a sanções disciplinares, que podem incluir advertência, suspensão, demissão por justa causa, além das responsabilizações civil, administrativa e criminal cabíveis.

9. Revisão a Atualização

Esta política será revisada periodicamente para assegurar sua atualização e conformidade com as melhores práticas e a legislação vigente.

10. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política de Integridade	Manual de Procedimentos	30/04/2025	1.0

Data	Descrição Ação	Versão	Responsável
30/04/2025	Elaboração	1.0	Jurídico
30/04/2025	Revisado e Aprovado	2.0	Diretoria Executiva

Política de Logs e Auditoria de Acessos

1. OBJETIVO

Estabelecer as diretrizes e responsabilidades para geração, armazenamento, análise e auditoria de logs de acesso e de eventos operacionais nos sistemas e plataformas da JB3 SOFTWARES S.A., garantindo rastreabilidade, integridade, disponibilidade e conformidade com a Lei nº 13.709/2018 (LGPD) e com as normas de segurança da informação e boas práticas de governança tecnológica adotadas pela organização.

2. ABRANGÊNCIA

Esta política aplica-se a todos os sistemas, APIs, bancos de dados, aplicações web e mobile, infraestruturas de nuvem e componentes tecnológicos sob gestão da JB3 SOFTWARES S.A., bem como aos produtos e serviços desenvolvidos e mantidos pela empresa.

3. VIGÊNCIA

Essa política passa a vigorar a partir da data da publicação.

4. DOCUMENTOS RELACIONADOS

MAN.001 - Manual do SGI

POL.000 - Política Integrada

POL.001 – Política de Segurança da Informação

5. DIRETRIZES

• Todos os acessos, consultas, autorizações, alterações e transmissões de dados devem

gerar registros de log contendo, no mínimo: usuário, data/hora, origem, operação executada, resultado e identificador da sessão.

• Os logs deverão ser armazenados em ambiente seguro e segregado, com controle de acesso restrito aos administradores autorizados e à área de Segurança da Informação.

• Os registros deverão ser protegidos contra alteração e exclusão indevida, utilizando mecanismos de integridade como hash criptográfico, WORM storage ou tecnologias equivalentes.

• O período mínimo de retenção dos logs será de 12 (doze) meses, podendo ser ampliado por exigência legal, contratual ou regulatória.

• O acesso aos logs será auditado, e toda consulta deverá ser registrada e vinculada a um usuário autenticado.

6. AUDITORIA E MONITORAMENTO

O Comitê de Segurança e Riscos realizará auditorias periódicas para verificar a conformidade desta política, avaliar a completude dos registros e identificar eventuais anomalias ou tentativas de manipulação. As trilhas de auditoria serão utilizadas para investigação de incidentes, auditorias internas e atendimento a solicitações formais de autoridades competentes ou clientes empresariais, conforme contratos vigentes.

7. AUDITORIA E MONITORAMENTO

• Diretoria Executiva – Aprovar esta política e garantir recursos para sua execução.

• Comitê de Segurança e Riscos – Monitorar a aplicação e revisar os controles periodicamente.

• Administradores de Sistemas – Implementar, revisar e manter os mecanismos de geração e proteção dos logs.

• DPO / Jurídico – Apoiar auditorias e garantir conformidade com a LGPD e demais normas aplicáveis.

8. CONFORMIDADE LEGAL E NORMATIVA

Esta política está alinhada às seguintes normas e boas práticas:

• Lei nº 13.709/2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

• ISO/IEC 27001:2022 – Segurança da Informação

• ISO/IEC 27701:2019 – Privacidade da Informação

• ISO 31000:2018 – Gestão de Riscos

• Boas práticas de governança corporativa e compliance da JB3 SOFTWARES S.A.

9. VIGÊNCIA E REVISÃO

Esta política entra em vigor na data de sua publicação e deverá ser revisada a cada 12 (doze) meses ou sempre que ocorrerem mudanças significativas na infraestrutura tecnológica, nos produtos ou nas exigências legais.

10. HISTÓRICO DE ALTERAÇÃO

Título	Subtítulo	Emissão	Versão
Política de Logs e Auditoria de Acesso	**Manual de Procedimentos**	**31/03/2025**	**1.0**

Data	Descrição Ação	Versão	Responsável
31/03/2025	**Elaboração**	**1.0**	**Jurídico**
28/04/2025	**Revisado e Aprovado**	**2.0**	**Diretoria Executiva**

Política de Privacidade e Proteção de Dados Pessoais

1. Introdução

Esta Política tem como objetivo informar como a JB3 SOFTWARES S.A. coleta, utiliza, armazena, compartilha e protege os dados pessoais de seus clientes, colaboradores, fornecedores, parceiros e demais titulares de dados, em conformidade com a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018).

2. Âmbito de Aplicação

Aplica-se a todos os dados pessoais tratados pela JB3 SOFTWARES S.A., em qualquer formato, seja eletrônico, físico ou outro meio.

3. Definições

Dados Pessoais: Informações relacionadas a pessoa natural identificada ou identificável.

Titular: Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

Tratamento: Qualquer operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, armazenamento, eliminação, entre outros.

4. Princípios

A JB3 SOFTWARES S.A. se compromete a tratar os dados pessoais observando os seguintes princípios:

Finalidade: Utilização dos dados para propósitos legítimos e específicos.

Adequação: Tratamento compatível com as finalidades informadas.

Necessidade: Limitação ao mínimo necessário para a finalidade.

Livre acesso: Garantia de acesso aos dados pelo titular.

Qualidade dos dados: Exatidão, clareza e atualização.

Segurança: Proteção contra acesso não autorizado, vazamento, perda ou alteração.

Transparência: Informações claras sobre o tratamento.

Prevenção: Adoção de medidas para evitar danos.

Não discriminação: Não uso dos dados para fins discriminatórios ilegais ou abusivos.

Responsabilização e prestação de contas.

5. Coleta e Uso dos Dados

5.1. Dados coletados:

Esta empresa coleta dados pessoais fornecidos diretamente pelo titular, como nome, CPF, endereço, telefone, e-mail, dados financeiros, dados de navegação, entre outros pertinentes aos serviços prestados.

5.2. Finalidades do tratamento:

Os dados são utilizados para atendimento ao cliente, execução de contratos, cumprimento de obrigações legais, melhorias nos serviços, marketing autorizado, entre outros objetivos legítimos.

6. Compartilhamento de Dados

A JB3 SOFTWARES S.A. poderá compartilhar dados pessoais com parceiros, fornecedores, autoridades públicas e demais terceiros, sempre observando a finalidade, a segurança e as bases legais previstas na LGPD.

7. Segurança da Informação

Esta empresa adota medidas técnicas e administrativas para proteger os dados pessoais contra acesso não autorizado, divulgação indevida, alteração, perda ou qualquer forma de tratamento inadequado.

8. Direitos dos Titulares

Os titulares dos dados possuem os seguintes direitos, podendo exercê-los mediante contato com a empresa:

Confirmação da existência de tratamento.

Acesso aos dados.

Correção de dados incompletos, inexatos ou desatualizados.

Anonimização, bloqueio ou eliminação de dados desnecessários ou excessivos.

Portabilidade dos dados a outro fornecedor.

Eliminação dos dados tratados com consentimento.

Informação sobre compartilhamento de dados.

Revogação do consentimento.

Reclamação junto à Autoridade Nacional de Proteção de Dados (ANPD).

9. Retenção dos Dados

Os dados pessoais serão mantidos pelo tempo necessário para cumprir as finalidades para as quais foram coletados, observadas obrigações legais e regulatórias.

10. Alterações na Política

Esta Política poderá ser atualizada para atender novas exigências legais ou mudanças nas práticas desta empresa, sendo divulgadas as alterações aos titulares.

11. Disposições Finais

Para mais informações ou para exercer seus direitos, o titular pode entrar em contato com a empresa através dos canais informados.

12. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política de Privacidade e Proteção de Dados Pessoais	**Manual de Procedimentos**	**31/03/2025**	**1.0**

Data	Descrição Ação	Versão	Responsável
31/03/2025	**Elaboração**	**1.0**	**Jurídico**
31/03/2025	**Revisado e Aprovado**	**2.0**	**Diretoria Executiva**

Política de Retenção de Dados e Auditoria de Longo Prazo

1. Objetivo

Estabelecer diretrizes para a retenção, integridade, rastreabilidade e auditoria de dados corporativos, garantindo conformidade com legislações aplicáveis e normas de segurança da informação.

2. Abrangência

Aplica-se a todos os dados armazenados e processados pela JB3 SOFTWARES S.A., incluindo dados pessoais, registros de sistema, trilhas de auditoria e documentos contratuais.

3. Retenção de Dados

- Os dados devem ser retidos pelo período mínimo exigido por lei ou contrato, conforme tabela de retenção definida pela área jurídica.
- Após o prazo de retenção, os dados devem ser descartados de forma segura, exceto quando sujeitos a armazenamento imutável.

4. Armazenamento Imutável

- Dados críticos, como trilhas de auditoria, logs de sistema e evidências de conformidade, devem ser armazenados em sistemas com **proteção contra alteração ou exclusão** (ex: WORM – Write Once, Read Many).
- O armazenamento imutável deve ser validado periodicamente por auditoria interna.

5. Trilhas de Auditoria de Longo Prazo

- O sistema deve gerar e manter trilhas de auditoria completas, com registros de acesso, alteração e exclusão de dados.
- Trilhas devem ser protegidas contra adulteração e acessíveis apenas por pessoal autorizado.
- A retenção mínima para trilhas de auditoria será de **5 anos**, salvo exigência legal superior.

6. Funcionalidades do Sistema

- O sistema deve possuir:
  - Geração automática de trilhas de auditoria.
  - Mecanismos de verificação de integridade dos dados.
  - Controle de acesso baseado em perfil.
  - Logs exportáveis para fins de auditoria externa.

7. Conformidade Legal e Normativa

- Esta política está alinhada com:
  - **Lei Geral de Proteção de Dados (LGPD)**
  - **ISO/IEC 27001 e 27018**
  - **Requisitos contratuais e regulatórios aplicáveis**

8. Revisão e Auditoria

- A política será revisada anualmente ou em caso de mudanças regulatórias.
- Auditorias internas e externas serão realizadas para verificar conformidade.

9. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política de Retenção de Dados e Auditoria de Longo Prazo	**Manual de Procedimentos**	**01/10/2025**	**1.0**

Data	Descrição Ação	Versão	Responsável
01/10/2025	**Elaboração**	**1.0**	**Jurídico**
01/10/2025	**Revisado e Aprovado**	**2.0**	**Diretoria Executiva**

Política de Segurança da Informação

1. Introdução

A segurança da informação desempenha um papel fundamental na preservação da confidencialidade, integridade e disponibilidade dos dados e informações da JB3 SOFTWARES S.A. Esta política estabelece diretrizes e princípios para assegurar a proteção adequada contra ameaças internas e externas.

2. Definição da Política de Segurança da Informação

A Política de Segurança da Informação define as medidas e práticas para garantir a segurança dos ativos de informação, abrangendo dados, sistemas, redes, e informações confidenciais relacionadas aos nossos clientes, colaboradores e parceiros.

3. Propósito

O propósito desta política é proteger a integridade, confidencialidade e disponibilidade dos dados da empresa, garantindo a conformidade com regulamentações, promovendo a confiança dos stakeholders e mitigando riscos relacionados à segurança da informação.

Estabelecer e orientar a obrigatoriedade da adoção de controles e processos para atendimento as premissas de segurança da informação.

Mitigar os riscos de incidentes, responsabilidade legal orientando colaboradores, clientes e parceiros.

Estar aderente as boas práticas estabelecidas por nossos clientes para garantir a confiabilidade em relação os serviços prestados.

4. Escopo

Esta política abrange todos os colaboradores, prestadores de serviços, sistemas ou indivíduos que operam através de serviços de inteligência da JB3 SOFTWARES S.A. Aplica-se a todas as formas de dados, independentemente do meio em que são armazenados ou processados.

5. Diretrizes e Princípios

Confidencialidade: Garantir que as informações transacionadas não sejam acessadas e após processamento sejam eliminadas automaticamente, eliminando a necessidade de tratativas manuais por colaboradores internos.

Integridade: Assegurar que as informações sejam precisas, completas e protegidas contra alterações não autorizadas no momento do processamento e extração das mesmas.

Disponibilidade: Garantir que as informações estejam disponíveis em tempo real em qualquer momento do processo.

6. Requisitos

- Utilização de senhas seguras e políticas de controle de acesso.
- Atualizações regulares de software e sistemas.
- Proteção contra malware e outras ameaças cibernéticas.
- Backup regular e recuperação de dados.
- Compartilhamento seguro de informações.
- Papéis e Responsabilidades
- Direção: Responsável pela aprovação e promoção da política.
- Gestores e Líderes de Equipe: Encarregados de garantir a implementação e conformidade na equipe.
- Colaboradores: Responsáveis por seguir as práticas de segurança estabelecidas.

A JB3 SOFTWARES S.A. estabelece a Diretoria e um colaborador como responsável pela Segurança da Informação como partes interessadas principais (stakeholders) na gestão de segurança da informação e responsáveis pela segurança da informação.

Diretoria e Responsável serão responsáveis pela:

- Análise, revisão, manutenção e proposição de aprovação de políticas e normas de segurança da informação, garantindo que estas estejam alinhadas com os objetivos estratégicos.
- Auditoria e implementação das políticas, normas e procedimentos, assegurando a aderência às melhores práticas e regulamentações pertinentes.
- Disponibilização dos recursos necessários para uma gestão efetiva de segurança da informação, incluindo tecnologia, treinamento e pessoal.
- Todas as atividades de segurança da informação estejam em conformidade com a política estabelecida.
- Divulgação e sensibilização sobre a política de segurança, promovendo uma cultura organizacional de segurança da informação.
- Identificação das mudanças nos riscos e necessidades de ações preventivas, priorizando ações com base em avaliações de riscos.
- Condução da gestão e operação da segurança da informação, baseando-se nas políticas e diretrizes estabelecidas pela Diretoria.

- Elaboração e evolução das normas e procedimentos de segurança da informação necessários, contribuindo para a eficácia da política de segurança.
- Gestão de incidentes de segurança da informação, assegurando um tratamento adequado.

Colaboradores serão responsáveis pela:

- Adesão ao cumprimento integral aos termos da Política Geral de Segurança da Informação, incluindo normas e procedimentos relacionados.
- Reportar à Diretoria ou Responsável de Segurança da informação qualquer evento que possa comprometer a segurança das informações ou dos recursos computacionais da JB3 SOFTWARES S.A.

7. Política para uso de dispositivos pessoais

A organização permite o uso de dispositivos pessoais para acessar sistemas corporativos, e para que isso ocorra, segue as seguintes regras:

- Autorização Prévia: Somente dispositivos autorizados pela equipe de segurança podem acessar o código fonte, no entanto, não há permissão de acesso ao banco de dados
- Segurança Mínima:
  - Senhas fortes e autenticação de dois fatores (2FA).
  - Criptografia de dados armazenados localmente.
  - Firewall e software de antivírus atualizado.
- Acesso aos Fontes das Aplicações:
  - Acesso Restrito: Dispositivos pessoais não devem permitir acesso aos bancos de dados de produção em hipótese alguma.
  - Máquina Virtual: Para garantir a gestão de alterações e atualização do código fonte, o acesso é permitido por meio de máquina virtual de forma a garantir a propriedade intelectual dos fontes e não permitir download para ambiente externo da máquina virtual.
  - Monitoramento e Controle: A organização utiliza mecanismos para acompanhamento, monitoramento e controle de acesso ao ambiente virtual.

- Procedimento de Desconexão: Em caso de desligamento ou mudança de função, o acesso a máquina virtual é desconectado remotamente de forma imediata.

8. Solução de IDS e IPS

Possuímos uma ferramenta de IDS (Intrusion Detection System) para monitorar o tráfego da rede e identifica atividades suspeitas, gerando alertas para as áreas responsáveis. Além disso, gerar bloqueios ou mitigar ataques em tempo real.

Esses sistemas apoiam na:

- Detectar acessos não autorizados antes que causem danos.
- Bloquear ataques como SQL Injection, DDoS e exploração de vulnerabilidades.
- Monitorar padrões de tráfego e detectar atividades anômalas.

Configuração e Monitoramento com Wazuh

Coleta de Dados e Logs

- O Wazuh deve coletar logs de:
  - Sistemas Operacionais (Syslog, Event Viewer).
  - Firewalls e IDS (ex.: Suricata, Snort).
  - Aplicações Críticas e APIs.
  - Atividades de usuários privilegiados.
- Logs são analisados em tempo real para detectar comportamentos anômalos.

Detecção de Ameaças (SIEM)

- Wazuh utiliza regras de correlação e inteligência de ameaças para gerar alertas em eventos como:
  - Tentativas de login suspeitas (*brute force*).
  - Execução de processos maliciosos.
  - Alterações em arquivos críticos do sistema.
  - Transferência de dados sensíveis.
- Alertas são categorizados por criticidade:

- 🔴 Crítico → Necessidade de resposta imediata.
- 🟠 Alto → Investigação urgente.
- 🟡 Médio/Baixo → Monitoramento contínuo.

9. Validade, Aprovação e Revisão

Esta política entra em vigor na data de aprovação e será revisada anualmente ou sempre que houver mudanças significativas na infraestrutura, regulamentações ou ameaças de segurança.

Essa política em cada atualização terá necessidade de aprovação dos sócios e responsáveis por segurança da informação.

10. Conformidade

A JB3 SOFTWARES S.A. compromete-se a cumprir todas as leis e regulamentações relacionadas à segurança da informação, incluindo normas setoriais aplicáveis.

11. Auditoria e Monitoramento

Serão realizadas auditorias regulares para garantir a conformidade com esta política. O monitoramento contínuo será implementado para identificar e responder rapidamente a possíveis incidentes de segurança.

Para garantir a eficácia e a segurança da informação, a JB3 SOFTWARES S.A. deve implementar e revisar periodicamente, a cada dois meses, uma série de planos de ação abrangendo medidas preventivas, corretivas, detectivas, repressivas e avaliativas. Essas ações são essenciais para manter a integridade e a segurança dos dados.

Auditoria de Novas Operações: No momento da aquisição de novas operações, é crucial realizar uma auditoria detalhada durante a fase inicial do projeto. Isso permitirá a identificação e avaliação de potenciais riscos, resultando na elaboração de um relatório de riscos. Com base neste relatório, devem ser tomadas as medidas necessárias para alinhar essas novas operações aos padrões de segurança estabelecidos.

Procedimentos de Propriedade Intelectual e Software: A implementação de procedimentos adequados é necessária para assegurar o cumprimento dos direitos de propriedade intelectual, bem como o uso correto de softwares proprietários. Este passo é fundamental para evitar violações legais e para proteger os ativos intelectuais da empresa.

Sistemas de Monitoramento: A JB3 SOFTWARES S.A. deverá estabelecer sistemas de monitoramento eficazes que abranjam estações de trabalho, servidores, e-mails, conexões à internet, dispositivos móveis ou wireless, e outros componentes da rede. Estes sistemas são cruciais para:

- Identificar e registrar usuários e seus respectivos acessos.
- Monitorar e documentar o manuseio de materiais e informações.

Divulgação de Informações Monitoradas: Em casos de exigências judiciais, a JB3 SOFTWARES S.A. poderá ser requerida a divulgar informações coletadas pelos sistemas de monitoramento e auditoria. Tal divulgação deve ser feita sob a orientação e aprovação de um gerente ou autoridade superior.

Inspeções Físicas: A JB3 SOFTWARES S.A. reserva o direito de realizar inspeções físicas em qualquer equipamento de sua propriedade, como parte de suas práticas de auditoria e monitoramento. Esta medida visa garantir a conformidade com as políticas de segurança da empresa e a detecção de possíveis ameaças ou vulnerabilidades.

Essas medidas, tomadas em conjunto, formam um quadro robusto de segurança da informação, assegurando que a JB3 SOFTWARES S.A. mantenha sua integridade operacional e proteja seus ativos de informação contra ameaças internas e externas. É fundamental que essas práticas sejam regularmente revisadas e atualizadas para responder a um ambiente em constante mudança e a ameaças emergentes.

12. Sanções e Punições

O não cumprimento desta política pode resultar em ações disciplinares, incluindo advertências, suspensões ou rescisões de contrato, conforme a gravidade da violação.

13. Casos Omissos

Situações não previstas nesta política serão analisadas caso a caso pela equipe de segurança da informação.

14. Glossário

- Confidencialidade:
  - Definição: Princípio de segurança que garante que as informações são acessadas apenas por pessoas autorizadas e que não são divulgadas indevidamente.
-
  - Definição: Princípio que assegura que as informações sejam precisas, completas e protegidas contra alterações não autorizadas.
-
  - Definição: Princípio que garante que as informações estejam disponíveis quando necessárias e que os sistemas estejam operacionais.

- Definição: Senhas que são complexas e difíceis de serem adivinhadas, geralmente combinando letras maiúsculas e minúsculas, números e caracteres especiais.

- Definição: Software malicioso projetado para causar danos a computadores, redes ou sistemas, incluindo vírus, worms, trojans e spyware.

- Definição: Processo de cópia de dados para prevenir a perda de informações e a capacidade de restaurar esses dados em caso de falha ou perda.

- Definição: Regulamentações específicas para uma determinada indústria ou setor, estabelecendo padrões e requisitos de segurança.

- Definição: Evento que compromete a segurança da informação, podendo envolver acessos não autorizados, perda de dados, entre outros.

- Definição: Medidas ou ações tomadas em resposta a violações de políticas, podendo incluir advertências, suspensões ou rescisões de contrato.

- Definição: Situações não previstas explicitamente na política, exigindo avaliação e decisões específicas conforme o contexto.

- Definição: Processo constante de observação e análise para identificar e responder rapidamente a possíveis ameaças ou incidentes de segurança.

15. Gestão da Política

A responsabilidade pela gestão desta política é atribuída à equipe de segurança da informação, que será responsável por manter, revisar e atualizar conforme necessário.

16. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política de Segurança da Informação	Manual de Procedimentos	31/04/2025	1.0

Data	Descrição Ação	Versão	Responsável
31/04/2025	Elaboração	1.0	Jurídico
31/04/2025	Revisado e Aprovado	2.0	Diretoria Executiva

POLÍTICA DE UTILIZAÇÃO, AQUISIÇÃO, DESCARTE E RECICLAGEM DE BENS DE INFORMÁTICA

1. Introdução

Estabelecer diretrizes para a utilização, aquisição, descarte e reciclagem de bens de informática na JB3 SOFTWARES S.A., assegurando a conformidade com:

- Portaria INMETRO nº 170/2019, que regulamenta a certificação compulsória de produtos da área de Tecnologia da Informação e Comunicação (TIC);

- Lei nº 12.305/2010 (Política Nacional de Resíduos Sólidos – PNRS) e Decreto nº 10.936/2022, que dispõem sobre a gestão de resíduos sólidos e logística reversa.

2. Âmbito de Aplicação

Esta política se aplica a todos os colaboradores, setores, fornecedores e prestadores de serviços envolvidos na utilização, aquisição, manutenção, gerenciamento, descarte e reciclagem de equipamentos de informática.

3. Base Legal

- Portaria INMETRO nº 170/2019;

- Lei nº 12.305/2010 – Política Nacional de Resíduos Sólidos;

- Decreto nº 10.936/2022 – Regulamenta a PNRS;

- Normas técnicas brasileiras aplicáveis.

4. Diretrizes

4.1. Aquisição de Equipamentos

- Todos os bens de informática adquiridos pela empresa devem possuir certificação válida conforme a Portaria INMETRO nº 170/2019.

- A área de compras deverá exigir dos fornecedores documentos comprobatórios de certificação e manter registros atualizados.

- Somente serão contratados fornecedores que possuam comprovação de conformidade técnica e que apresentem plano ou certificado de destinação final ambientalmente adequada para equipamentos substituídos.

4.2. Utilização de Equipamentos

- Apenas equipamentos certificados pelo INMETRO poderão ser utilizados.

- Equipamentos fora de certificação deverão ser substituídos ou avaliados pelo setor de TI.

- O setor de TI será responsável por monitorar a conformidade e funcionamento, identificando e reportando irregularidades.

4.3. Manutenção e Controle

- A manutenção dos bens de informática deve respeitar as especificações técnicas e certificações vigentes.

- Todos os registros de manutenção e certificação devem ser mantidos atualizados pelo setor responsável.

4.4. Descarte, Reciclagem e Logística Reversa

- O descarte de bens de informática deverá seguir os princípios da Lei nº 12.305/2010, priorizando reutilização, reciclagem e, em último caso, destinação final ambientalmente adequada.
- Equipamentos obsoletos ou inservíveis deverão ser encaminhados para empresas ou cooperativas de reciclagem licenciadas, com emissão de certificado de destinação final.
- Sempre que possível, equipamentos em condições de uso poderão ser doados para instituições de interesse social, com registro formal da doação.
- O armazenamento temporário de equipamentos destinados ao descarte deverá ser feito em local apropriado, seguro e sinalizado, evitando contaminação ambiental.
- A empresa manterá registros anuais dos volumes e destinos dos resíduos eletrônicos gerados.

5. Responsabilidades

- Setor de Compras: Garantir a aquisição de equipamentos certificados e exigir dos fornecedores comprovação de destinação ambiental adequada para os equipamentos substituídos.

- Setor de Tecnologia da Informação (TI): Monitorar conformidade, gerenciar inventário e indicar equipamentos para descarte ou doação.

- Setor de Sustentabilidade ou Meio Ambiente (quando aplicável): Coordenar a logística reversa, controlar a destinação final e manter registros de comprovação.

- Colaboradores: Utilizar apenas equipamentos autorizados e seguir procedimentos internos para devolução e descarte.

6. Penalidades

O descumprimento desta política poderá acarretar medidas administrativas internas e responsabilização conforme legislação ambiental, incluindo advertências, suspensão e responsabilizações cíveis e criminais.

7. Revisão e Atualização

Esta política será revisada periodicamente para assegurar sua atualização e conformidade com as melhores práticas e a legislação vigente.

8. Informações e Revisões do Documento

Título	Subtítulo	Emissão	Versão
Política de Utilização, Aquisição, Descarte e Reciclagem de Bens de Informática	**Manual de Procedimentos**	**30/04/2025**	**1.0**

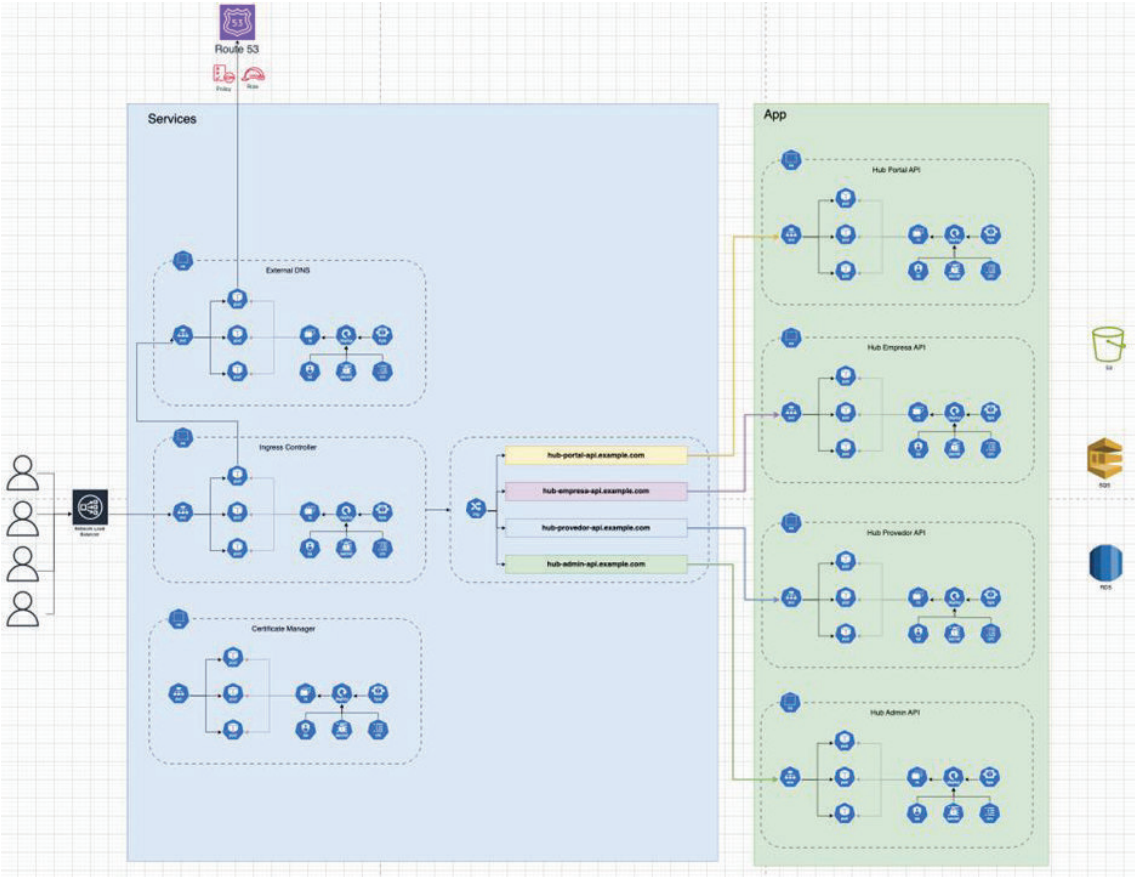
Data	Descrição Ação	Versão	Responsável
30/04/2025	**Elaboração**	**1.0**	**Jurídico**
30/04/2025	**Revisado e Aprovado**	**2.0**	**Diretoria Executiva**

1. Descrição

A solução oferece capacidade de auto scaling para ajustar recursos de forma dinâmica conforme a demanda, garantindo alta disponibilidade e performance. Conta com mecanismos robustos de disaster recovery para assegurar continuidade operacional em cenários críticos. Além disso, disponibiliza controle de acesso granular, permitindo definir permissões detalhadas por usuário ou grupo, aliado a logs e trilhas completas para auditoria e conformidade.

2. Auto scaling, disaster recovery

Para implementação da escalabilidade e resiliência fazemos uso do Kubernates, 100% integrado com mecanismos de segurança como firewall, waf, entre outros. A Firewall e o WAF usados são da AWS.



O Disaster Recovery, está implementado em modo HOT estando garantindo a distribuição do Kubernets e do Banco de dados em pelo menos duas Zonas distintas da AWS. Os componentes S3 e SQS já implementam nativamente Alta Disponibilidade e Disaster Recovery. Esta arquitetura, garante o Load Balance (LB - balanceamento), High-Availablity (HA – alta disponibilidade) e Disaster Recovery (DR – recuperação de desastres).

Adicionalmente a esta arquitetura, encontrase configurado toda a estrutura em Terraform, para levantamento do ambiente em modo COLD em qualquer outra região da AWS ou mesmo fora do Brasil para situação emergencial critica.

```
bash-3.2$ terraform init
Initializing the backend...
Initializing modules...
Initializing provider plugins...
- Reusing previous version of hashicorp/helm from the dependency lock file
- Reusing previous version of hashicorp/kubernetes from the dependency lock file
- Reusing previous version of hashicorp/aws from the dependency lock file
- Reusing previous version of hashicorp/tls from the dependency lock file
- Reusing previous version of hashicorp/random from the dependency lock file
- Reusing previous version of hashicorp/null from the dependency lock file
- Reusing previous version of hashicorp/cloudinit from the dependency lock file
- Using previously-installed hashicorp/tls v4.1.0
- Using previously-installed hashicorp/random v3.7.2
- Using previously-installed hashicorp/null v3.2.4
- Using previously-installed hashicorp/cloudinit v2.3.7
- Using previously-installed hashicorp/helm v3.0.2
- Using previously-installed hashicorp/kubernetes v2.38.0
- Using previously-installed hashicorp/aws v5.100.0

Terraform has been successfully initialized!

You may now begin working with Terraform. Try running "terraform plan" to see
any changes that are required for your infrastructure. All Terraform commands
should now work.

If you ever set or change modules or backend configuration for Terraform,
rerun this command to reinitialize your working directory. If you forget, other
commands will detect it and remind you to do so if necessary.
bash-3.2$ terraform output
eks_cluster_name = "gcc-tst-eks"
eks_nodes_sg_id = [
  "sg-0a4b9aa105ad4c16d",
]
eks_oidc_issuer_url = "https://oidc.eks.us-east-1.amazonaws.com/id/574A4B097775F457FFC822C5EA868665"
eks_oidc_thumbprint = "9e99a48a9960b14926bb7f3b02e22da2b0ab7280"
elasticache_auth_token = <sensitive>
elasticache_cluster_address = [
  "master.gcc-tst-redis-replication-group.za3zsr.use1.cache.amazonaws.com",
]
elasticache_cluster_arn = [
  "arn:aws:elasticache:us-east-1:018535004794:replicationgroup:gcc-tst-redis-replication-group",
]
elasticache_cluster_port = [
  6379,
]
irsa_sqs_role_arn = "arn:aws:iam::018535004794:role/gcc-tst-irsa-sqs"
rds_db_name = ""
rds_endpoint = "gcc-tst-rds-postgres.cc34y8wkctt2.us-east-1.rds.amazonaws.com:5432"
rds_password = <sensitive>
rds_port = 5432
rds_username = "adminuser"
s3_bucket_arn = {
  "gcc-tst-hub-files" = "arn:aws:s3:::gcc-tst-hub-files"
  "gcc-tst-logs-sqs" = "arn:aws:s3:::gcc-tst-logs-sqs"
}
s3_bucket_endpoint = {
  "gcc-tst-hub-files" = "gcc-tst-hub-files.s3.amazonaws.com"
  "gcc-tst-logs-sqs" = "gcc-tst-logs-sqs.s3.amazonaws.com"
}
sqs_queue_arn = [
  "arn:aws:sqs:us-east-1:018535004794:gcc-tst-dlq",
  "arn:aws:sqs:us-east-1:018535004794:gcc-tst-gerador-hash",
  "arn:aws:sqs:us-east-1:018535004794:gcc-tst-hash-consumer",
  "arn:aws:sqs:us-east-1:018535004794:gcc-tst-notifications",
  "arn:aws:sqs:us-east-1:018535004794:update-cache",
]
sqs_queue_name = [
  "gcc-tst-dlq",
  "gcc-tst-gerador-hash",
  "gcc-tst-hash-consumer",
  "gcc-tst-notifications",
  "update-cache",
]
sqs_queue_url = [
  "https://sqs.us-east-1.amazonaws.com/018535004794/gcc-tst-dlq",
  "https://sqs.us-east-1.amazonaws.com/018535004794/gcc-tst-gerador-hash",
  "https://sqs.us-east-1.amazonaws.com/018535004794/gcc-tst-hash-consumer",
  "https://sqs.us-east-1.amazonaws.com/018535004794/gcc-tst-notifications",
  "https://sqs.us-east-1.amazonaws.com/018535004794/update-cache",
]
bash-3.2$
```

3. Arquitetura

1. Disponibilidade e Continuidade Operacional

A arquitetura da plataforma foi concebida para garantir alta disponibilidade (HA) e continuidade de serviço em conformidade com as melhores práticas da AWS Well-Architected Framework.

Os principais mecanismos implementados são os seguintes:

1.1. Disaster Recovery (Recuperação de Desastres)

• O ambiente encontra-se implementado em modo HOT DR, com distribuição automática dos clusters Kubernetes e das instâncias de banco de dados em múltiplas Availability Zones (AZs) da AWS, garantindo redundância geográfica e tolerância a falhas.

• Os serviços Amazon S3 e Amazon SQS contam com replicação e recuperação de desastres nativa, assegurando a persistência e integridade dos dados em caso de incidentes críticos.
• Adicionalmente, a infraestrutura é definida em Terraform (Infraestrutura como Código), permitindo o provisionamento rápido em modo COLD DR em qualquer outra região AWS — ou até mesmo fora do território nacional — em situações de contingência severa.
1.2. Balanceamento de Carga (Load Balancing)
• Todos os componentes da plataforma implementam mecanismos de balanceamento de carga para otimização de desempenho e continuidade de serviço.
• Os portais, APIs e microserviços são balanceados via Kubernetes (Ingress Controller), que utiliza o AWS Network Load Balancer (NLB) para distribuir o tráfego de forma eficiente e segura.
• Os serviços RDS, SQS e S3 utilizam balanceamento nativo da AWS, garantindo distribuição inteligente de requisições e resiliência a picos de carga.
1.3. Alta Disponibilidade (High Availability)
• Todos os componentes críticos são configurados em modo redundante.
• A camada de aplicação, os serviços e APIs estão em pods replicados no Kubernetes, enquanto o banco de dados e demais serviços AWS (SQS, S3) contam com mecanismos automáticos de failover.
• Monitorização contínua e métricas de saúde garantem que qualquer instância degradada seja automaticamente substituída.

2. Escalabilidade e Performance
A plataforma foi desenhada para crescer horizontal e verticalmente, adaptando-se automaticamente à variação da carga de trabalho.
2.1. Auto Scaling
• O Kubernetes Horizontal Pod Autoscaler (HPA) está configurado para escalar automaticamente os pods quando a utilização atinge 75% de carga, permitindo o crescimento antes da saturação do sistema.
• O Cluster Autoscaler garante a criação de novos nós (nodes) de forma dinâmica, assegurando disponibilidade mesmo durante picos de tráfego.
2.2. Escalabilidade de Serviços AWS
• Amazon SQS e Amazon S3 implementam escalabilidade horizontal nativa, suportando alto débito e elevada concorrência sem necessidade de intervenção manual.
• O Amazon RDS encontra-se configurado com auto scaling de armazenamento e monitorização de métricas de CPU e memória, permitindo o aumento automático da capacidade conforme o crescimento da demanda.

2.3. Monitorização e Observabilidade
• O ambiente é monitorizado em tempo real através do Amazon CloudWatch, com alarmes proativos configurados para métricas de desempenho, capacidade e disponibilidade.
• Logs e métricas são agregados e analisados periodicamente para ajustes de performance e otimização de custos.

3. Segurança e Conformidade

A plataforma adota uma abordagem "Security by Design", garantindo a proteção de dados, comunicações e infraestrutura desde o desenvolvimento até a operação.

3.1. Proteção de Dados

• Dados em trânsito: protegidos com TLS 1.3 (TLS_AES_256_GCM_SHA384) em todas as comunicações externas e internas.

• Dados em repouso: criptografados via AWS KMS (Key Management Service), abrangendo S3, SQS e RDS, com gestão centralizada de chaves e rotação automática.

3.2. Proteção de Aplicações e APIs

• Implementação do AWS Web Application Firewall (WAF) para defesa contra ameaças em camada de aplicação, incluindo:

o SQL Injection

o Cross-Site Scripting (XSS)

o Remote File Inclusion

o Brute Force e ataques automatizados

• Integração com AWS Shield para proteção avançada contra:

o DDoS volumétricos

o Protocol Attacks (SYN Flood, ACK Flood, Fragmentation)

o Reflection/Amplification Attacks

3.3. Segurança de Rede

• Segmentação lógica das redes por ambiente (produção, homologação, desenvolvimento), garantindo isolamento total entre camadas.

• Security Groups e Network ACLs configurados com princípio de privilégio mínimo, restringindo comunicações a portas e IPs específicos.

• Integração com VPC Endpoints para comunicações seguras com serviços internos da AWS sem exposição pública.

3.4. Segurança no Ciclo de Desenvolvimento

• Processo de CI/CD seguro, com:

o Repositórios Git isolados e segregados por ambiente.

o Pipelines automatizados com validações de código, testes e escaneamento de vulnerabilidades.

o Deploy controlado com validação de integridade e rollback automático em caso de falha.

4. Conclusão

A arquitetura descrita combina resiliência operacional, elasticidade e segurança avançada, assegurando:

• Alta disponibilidade e recuperação automática de falhas;

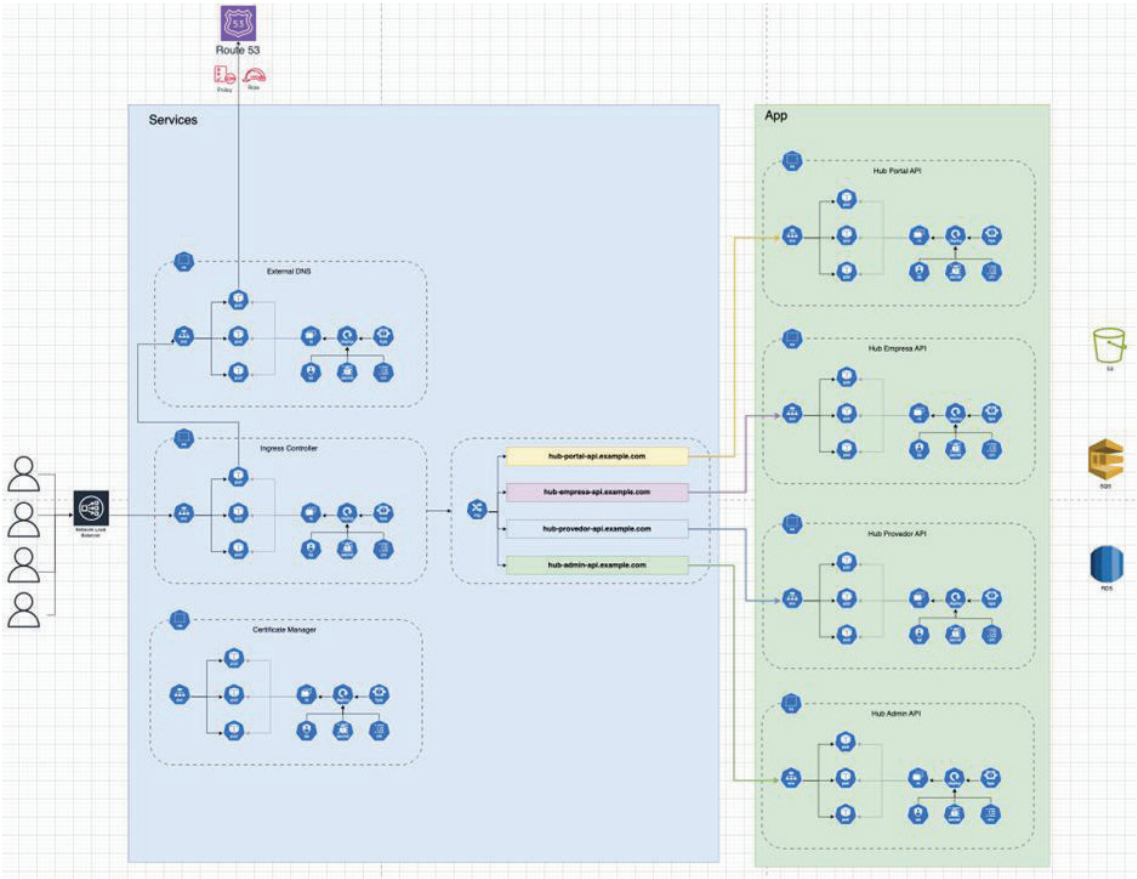
• Escalabilidade contínua e sob demanda;

• Proteção integral contra ameaças de rede e aplicação;

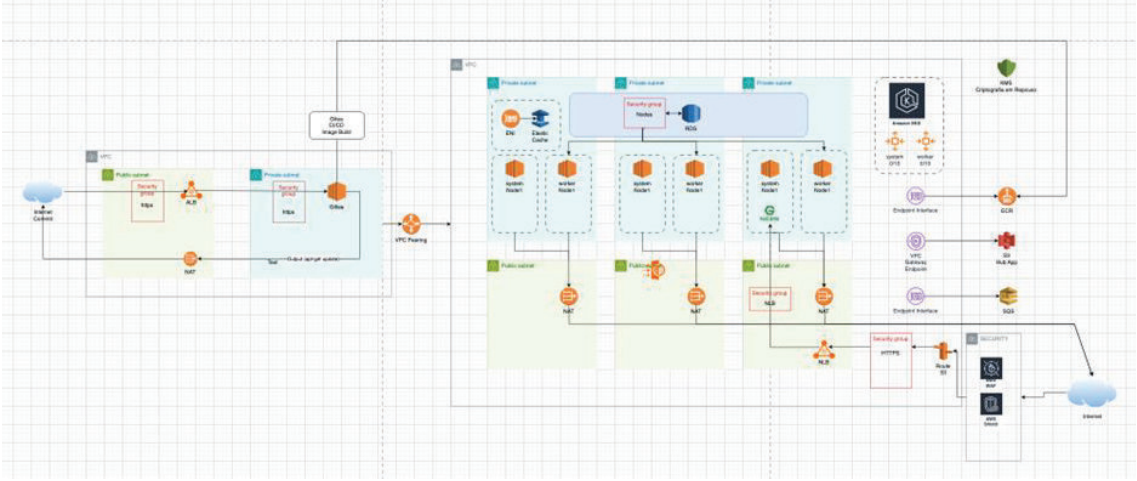
• Conformidade com os princípios da AWS Well-Architected Framework (Pilares de Reliability, Performance Efficiency e Security).

Esta combinação garante que a plataforma se mantém disponível, segura e eficiente mesmo sob cenários de alta carga, falhas regionais ou ameaças externas.

Para implementação da escalabilidade e resiliência fazemos uso do Kubernates, 100% integrado com mecanismos de segurança como firewall, waf, entre outros. A Firewall e o WAF usados são da AWS.



Abaixo detalhamos, a arquitetura que permite a escalabilidade, segurança e resiliência de cada um dos Hubs implementados.

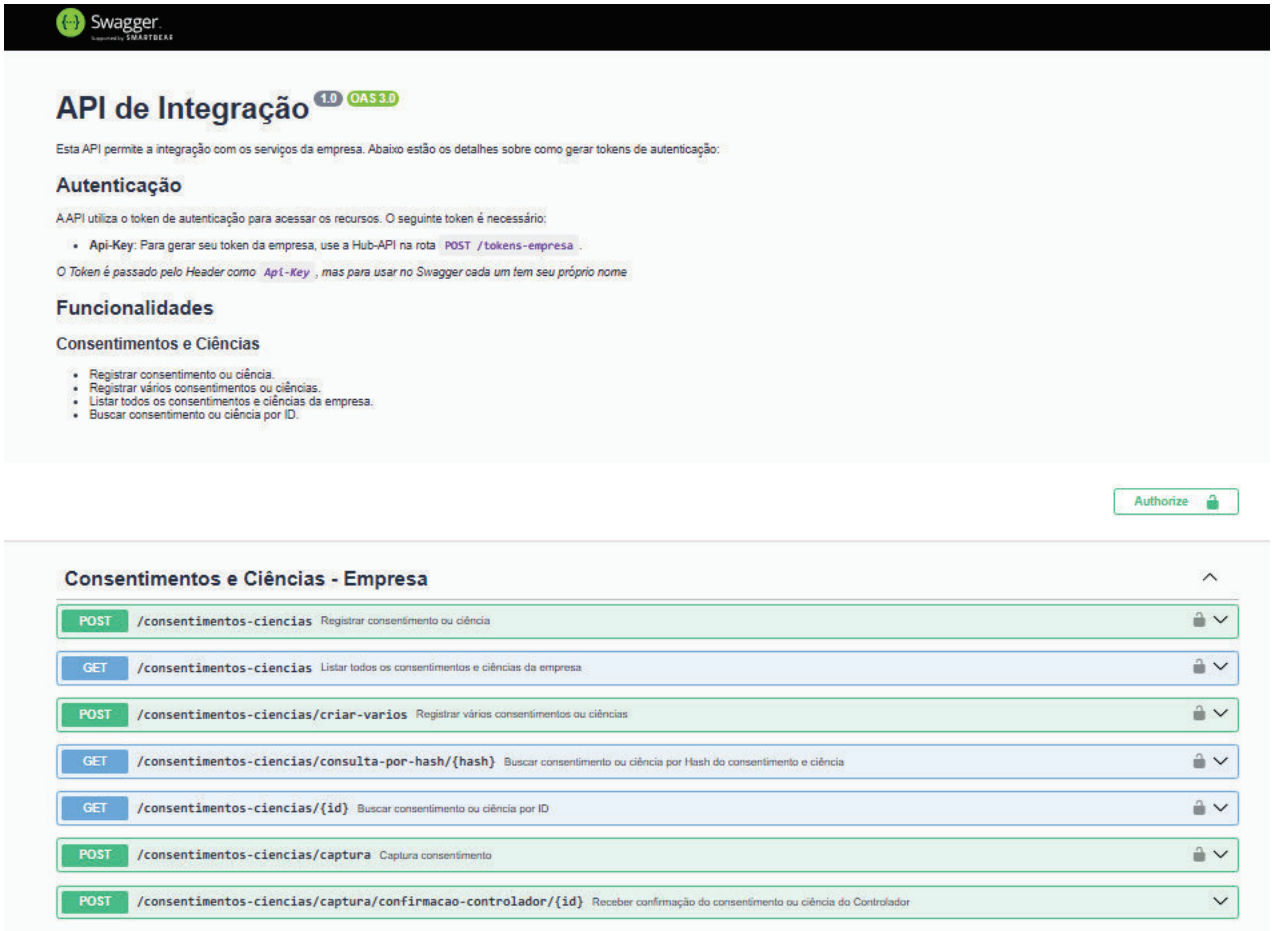


4. Swagger/OpenAPI

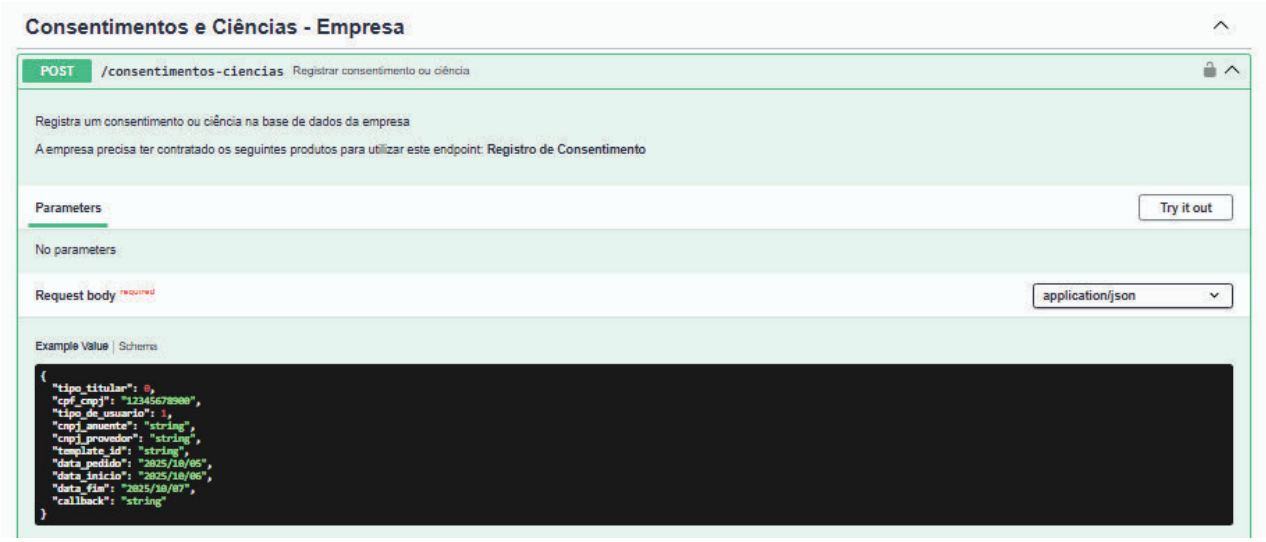
O Swagger da API Company possui um conjunto de ferramentas que facilita a documentação,
teste e integração de APIs REST. Ele utiliza a especificação OpenAPI, um padrão aberto para
descrever APIs de forma estruturada e legível tanto por humanos quanto por máquinas.

Abaixo prints dos endpoints da nossa API:

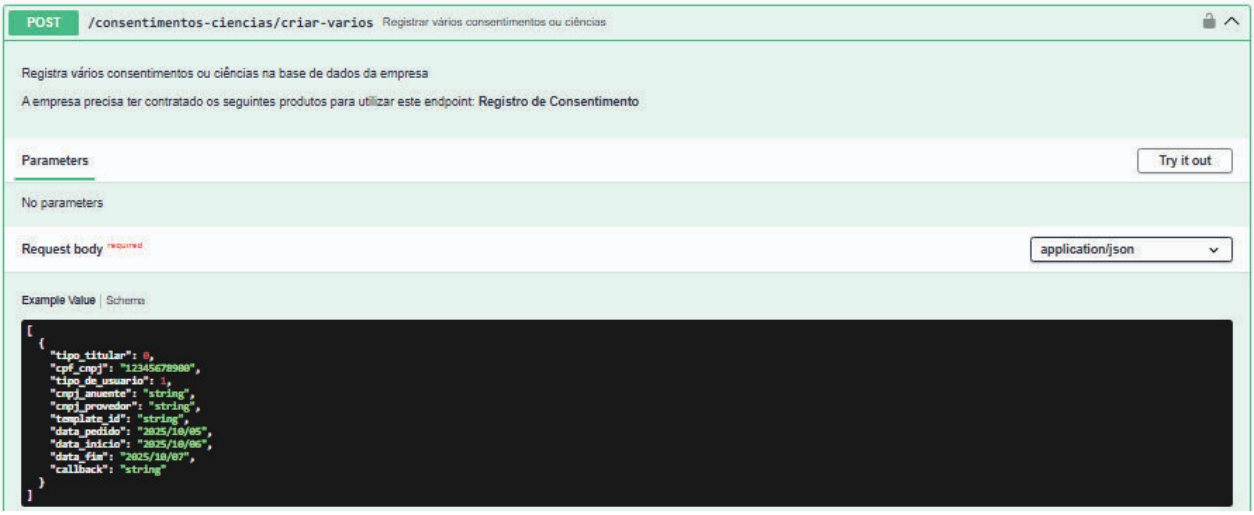
Link https://company.hml.quemmeviu.com.br/api



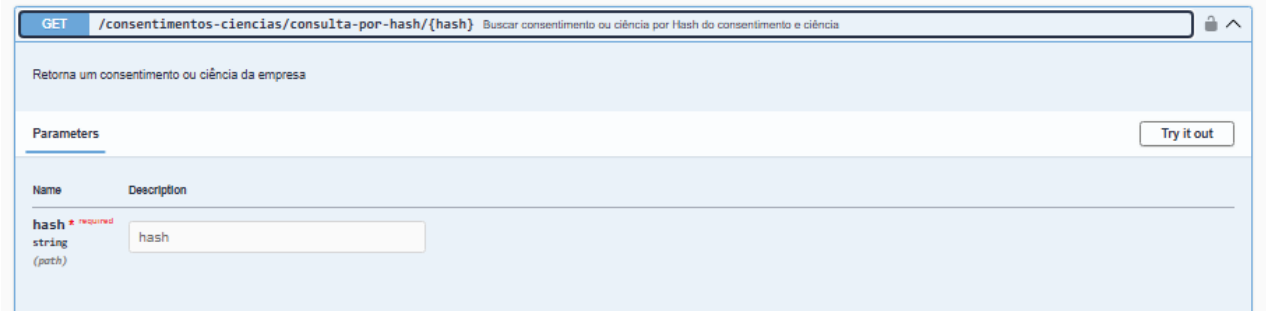
API Registro de consentimento e ciência



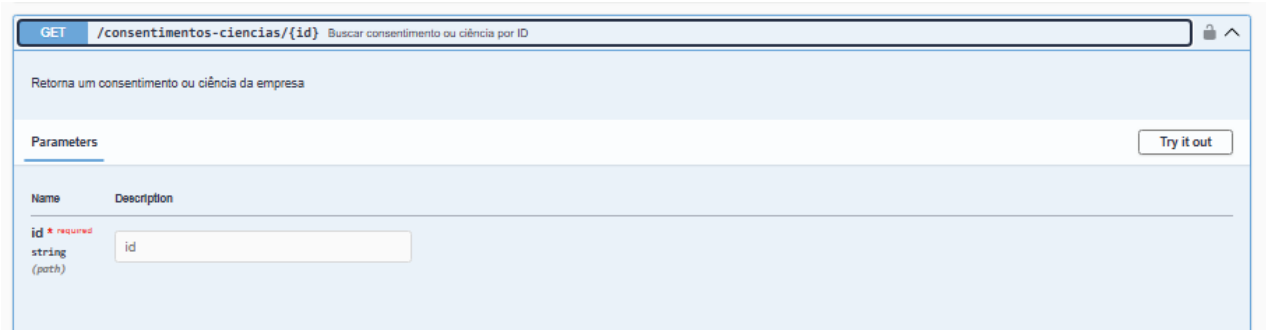
API registro de consentimento e ciência (vários)



API consulta pro meio do Hash



API consulta por meio do ID



API captura de consentimento

5. HISTÓRICO DE ALTERAÇÃO

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

1. Descrição

A solução visa garantir que as aplicações da GCC possam integrar-se de forma eficiente com sistemas internos e externos por meio de APIs robustas, escaláveis e seguras. Essa capacidade permite:
• Interoperabilidade entre diferentes plataformas e serviços.
• Escalabilidade, suportando aumento de carga e volume de dados sem comprometer desempenho.
• Segurança, assegurando proteção contra acessos não autorizados, vazamento de dados e ataques, utilizando práticas como autenticação, autorização e criptografia.
• Padronização, seguindo boas práticas de arquitetura (REST) e documentação clara para facilitar manutenção e evolução.

2. Arquitetura

1. Disponibilidade e Continuidade Operacional

A arquitetura da plataforma foi concebida para garantir alta disponibilidade (HA) e continuidade de serviço em conformidade com as melhores práticas da AWS Well-Architected Framework.

Os principais mecanismos implementados são os seguintes:

1.1. Disaster Recovery (Recuperação de Desastres)
• O ambiente encontra-se implementado em modo HOT DR, com distribuição automática dos clusters Kubernetes e das instâncias de banco de dados em múltiplas Availability Zones (AZs) da AWS, garantindo redundância geográfica e tolerância a falhas.
• Os serviços Amazon S3 e Amazon SQS contam com replicação e recuperação de desastres nativa, assegurando a persistência e integridade dos dados em caso de incidentes críticos.
• Adicionalmente, a infraestrutura é definida em Terraform (Infraestrutura como Código), permitindo o provisionamento rápido em modo COLD DR em qualquer outra região AWS — ou até mesmo fora do território nacional — em situações de contingência severa.

1.2. Balanceamento de Carga (Load Balancing)
• Todos os componentes da plataforma implementam mecanismos de balanceamento de carga para otimização de desempenho e continuidade de serviço.
• Os portais, APIs e microserviços são balanceados via Kubernetes (Ingress Controller), que utiliza o AWS Network Load Balancer (NLB) para distribuir o tráfego de forma eficiente e segura.
• Os serviços RDS, SQS e S3 utilizam balanceamento nativo da AWS, garantindo distribuição inteligente de requisições e resiliência a picos de carga.

1.3. Alta Disponibilidade (High Availability)
• Todos os componentes críticos são configurados em modo redundante.
• A camada de aplicação, os serviços e APIs estão em pods replicados no Kubernetes, enquanto o banco de dados e demais serviços AWS (SQS, S3) contam com mecanismos automáticos de failover.

• Monitorização contínua e métricas de saúde garantem que qualquer instância degradada seja automaticamente substituída.

3. Escalabilidade e Performance

A plataforma foi desenhada para crescer horizontal e verticalmente, adaptando-se automaticamente à variação da carga de trabalho.

3.1. Auto Scaling
• O Kubernetes Horizontal Pod Autoscaler (HPA) está configurado para escalar automaticamente os pods quando a utilização atinge 75% de carga, permitindo o crescimento antes da saturação do sistema.
• O Cluster Autoscaler garante a criação de novos nós (nodes) de forma dinâmica, assegurando disponibilidade mesmo durante picos de tráfego.

3.2. Escalabilidade de Serviços AWS
• Amazon SQS e Amazon S3 implementam escalabilidade horizontal nativa, suportando alto débito e elevada concorrência sem necessidade de intervenção manual.
• O Amazon RDS encontra-se configurado com auto scaling de armazenamento e monitorização de métricas de CPU e memória, permitindo o aumento automático da capacidade conforme o crescimento da demanda.

3.3. Monitorização e Observabilidade
• O ambiente é monitorizado em tempo real através do Amazon CloudWatch, com alarmes proativos configurados para métricas de desempenho, capacidade e disponibilidade.
• Logs e métricas são agregados e analisados periodicamente para ajustes de performance e otimização de custos.

4. Segurança e Conformidade

A plataforma adota uma abordagem "Security by Design", garantindo a proteção de dados, comunicações e infraestrutura desde o desenvolvimento até a operação.

4.1. Proteção de Dados
• Dados em trânsito: protegidos com TLS 1.3 (TLS_AES_256_GCM_SHA384) em todas as comunicações externas e internas.
• Dados em repouso: criptografados via AWS KMS (Key Management Service), abrangendo S3, SQS e RDS, com gestão centralizada de chaves e rotação automática.

4.2. Proteção de Aplicações e APIs
• Implementação do AWS Web Application Firewall (WAF) para defesa contra ameaças em camada de aplicação, incluindo:

o SQL Injection
o Cross-Site Scripting (XSS)

o Remote File Inclusion
o Brute Force e ataques automatizados
o Integração com AWS Shield para proteção avançada contra:
o DDoS volumétricos
o Protocol Attacks (SYN Flood, ACK Flood, Fragmentation)
o Reflection/Amplification Attacks

4.3. Segurança de rede

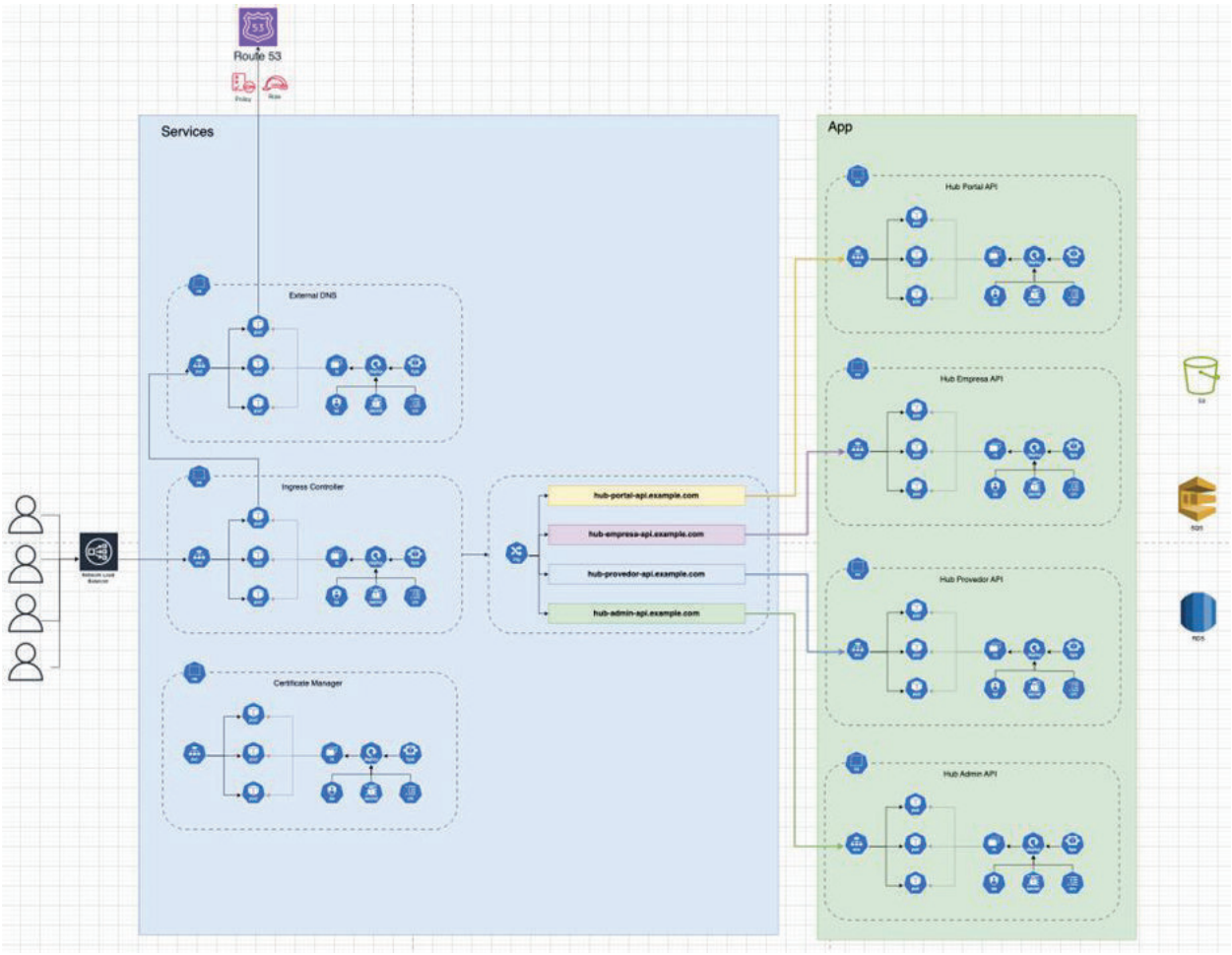
• Segmentação lógica das redes por ambiente (produção, homologação, desenvolvimento), garantindo isolamento total entre camadas.
• Security Groups e Network ACLs configurados com princípio de privilégio mínimo, restringindo comunicações a portas e IPs específicos.
• Integração com VPC Endpoints para comunicações seguras com serviços internos da AWS sem exposição pública.

4.4. Segurança no Ciclo de Desenvolvimento
• Processo de CI/CD seguro, com:
o Repositórios Git isolados e segregados por ambiente.
o Pipelines automatizados com validações de código, testes e escaneamento de vulnerabilidades.
o Deploy controlado com validação de integridade e rollback automático em caso de falha.

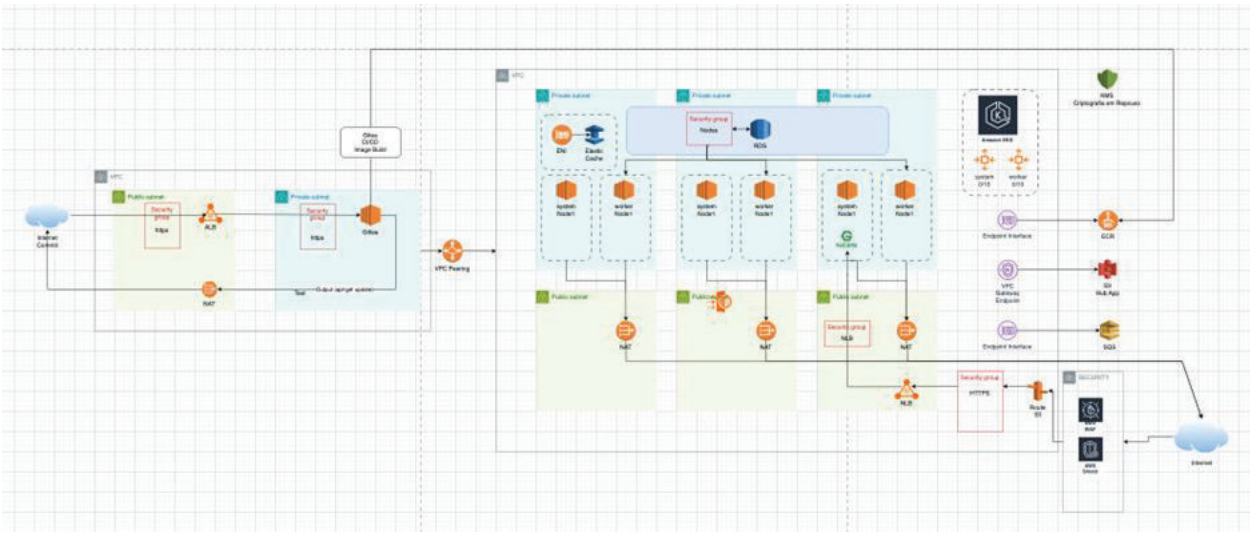
5. Conclusão

A arquitetura descrita combina resiliência operacional, elasticidade e segurança avançada, assegurando:
• Alta disponibilidade e recuperação automática de falhas;
• Escalabilidade contínua e sob demanda;
• Proteção integral contra ameaças de rede e aplicação;
• Conformidade com os princípios da AWS Well-Architected Framework (Pilares de Reliability, Performance Efficiency e Security).

Esta combinação garante que a plataforma se mantém disponível, segura e eficiente mesmo sob cenários de alta carga, falhas regionais ou ameaças externas.



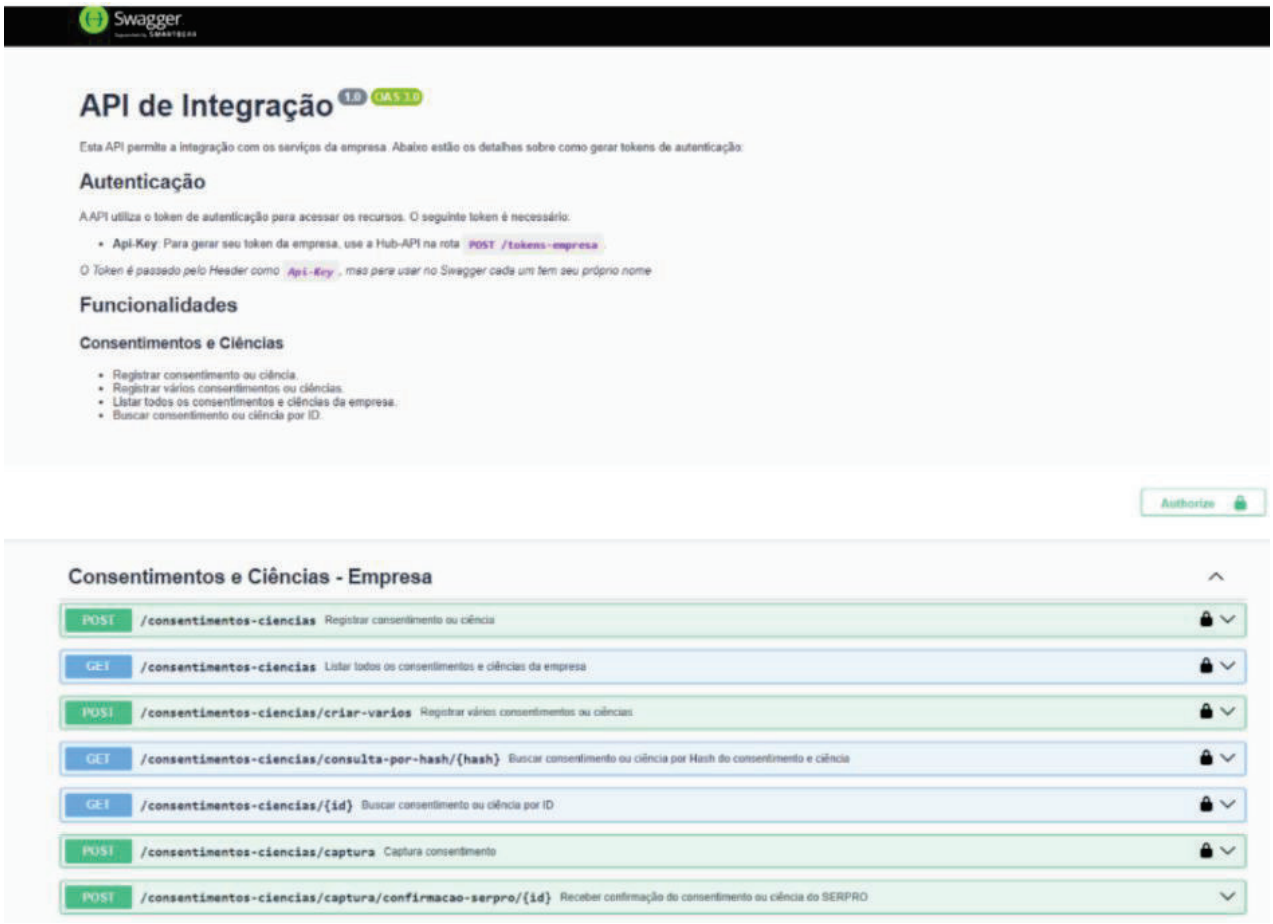
Abaixo detalhamos, a arquitetura que permite a escalabilidade, segurança e resiliência de cada um dos Hubs implementados.



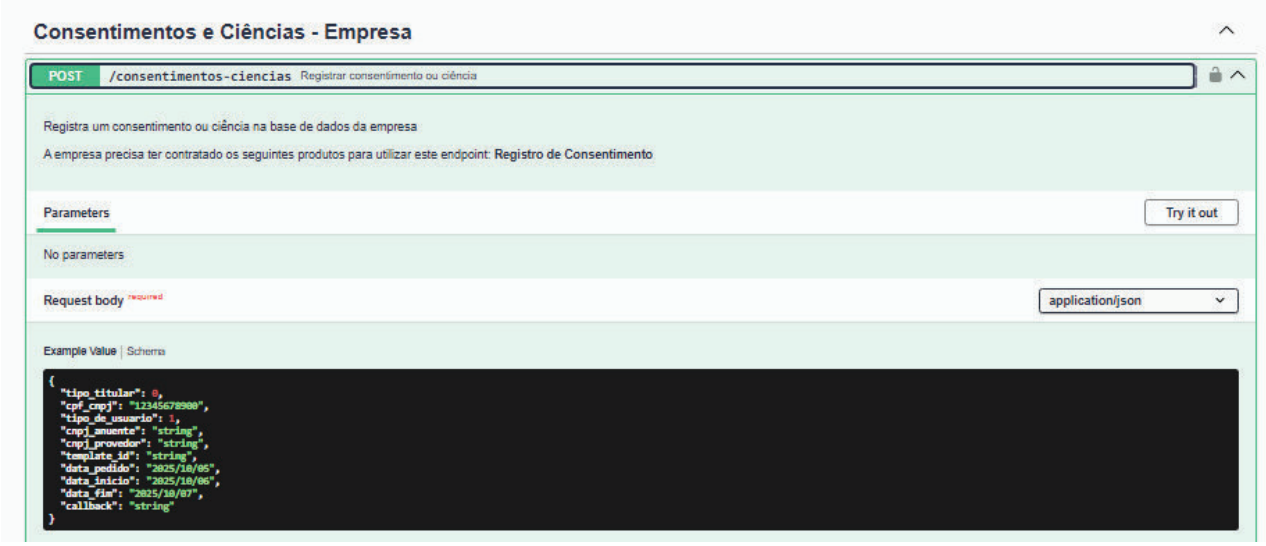
6. Swagger/OpenAPI

O Swagger da API Company possui um conjunto de ferramentas que facilita a documentação, teste e integração de APIs REST. Ele utiliza a especificação OpenAPI, um padrão aberto para descrever APIs de forma estruturada e legível tanto por humanos quanto por máquinas.

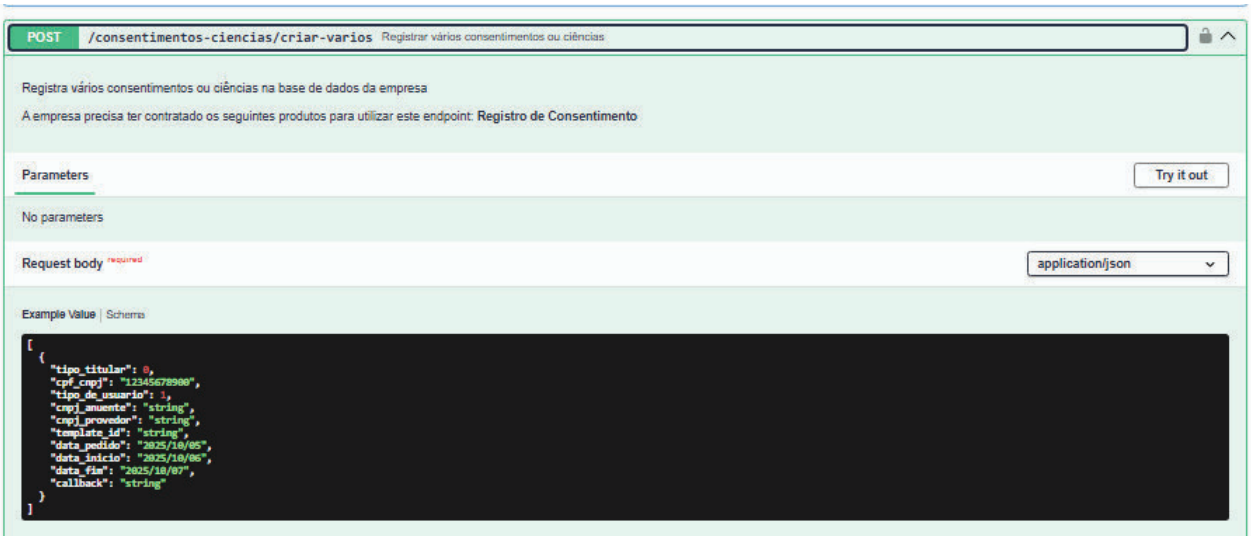
Abaixo prints dos endpoints da nossa API:



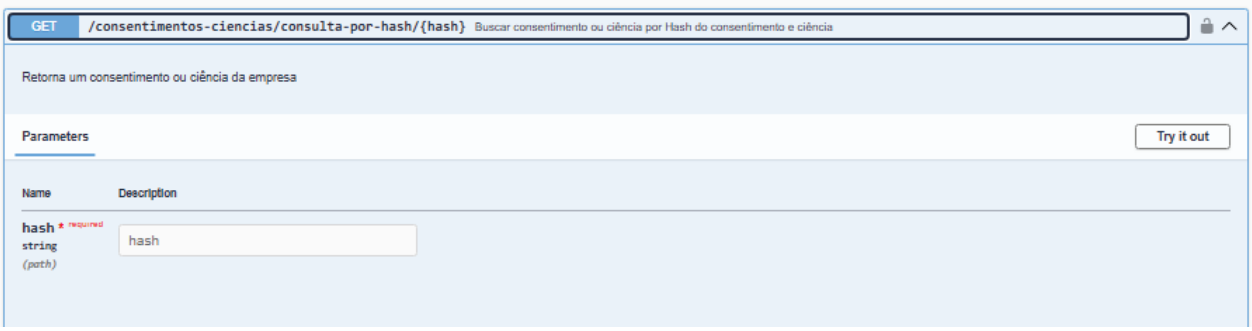
API Registro de consentimento e ciência



API registro de consentimento e ciência (vários)

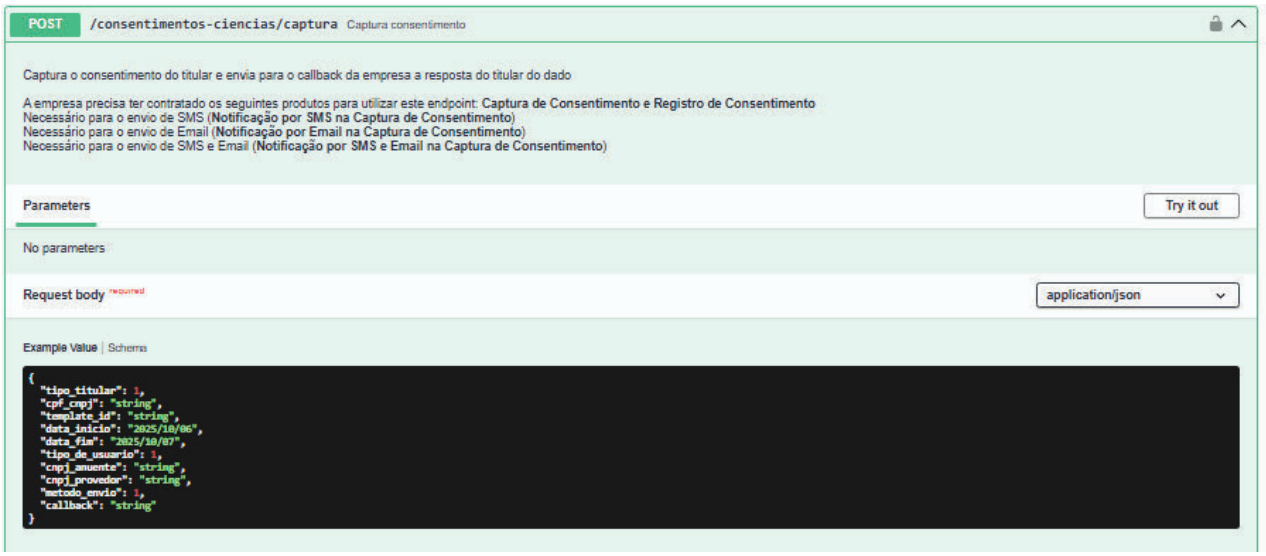


API consulta por meio do Hash



API consulta por meio do ID

API captura de consentimento



7. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

1. Descrição

A publicação do DPO (Data Protection Officer) no site institucional da JB3 Software é fundamental para garantir transparência e conformidade com a Lei Geral de Proteção de Dados (LGPD).
Essa prática demonstra o compromisso da empresa com a proteção de dados pessoais, facilita a comunicação com titulares e autoridades, e assegura que exista um canal oficial para esclarecimentos e solicitações relacionadas à privacidade e segurança da informação.

2. Evidência

O site institucional da JB3, cujo URL é https://jb3ti.com.br/ apresenta o contato do DPO:

3. Histórico de alterações

VERSÃO	DATA	NOME	AÇÃO (Elaboração, Revisão, Atualização, Aprovação)	CONTEÚDO
1.0	20/10/2025	Polyana Silva	Elaboração	Primeira versão
		Renato Pedroso	Aprovação	

REQUERIMENTO NOS TERMOS DO CREDENCIAMENTO Nº 390004-01/2025 – PORTARIA SENATRAN Nº 139/2025

À Secretaria Nacional de Trânsito – SENATRAN
Ministério dos Transportes

Assunto: Envio de Evidências Técnicas

JB3 SOFTWARES S.A., pessoa jurídica de direito privado, inscrita no CNPJ/MF 58.493.015/0001-19, sediada à Avenida Paulista nº 2300, Piso Pilotis, Sala 43, Ed. São Luís Gonzaga, Bela Vista, São Paulo – SP, CEP 01310-300, neste ato representada por sua representante legal, Sra. **ETELVINA DE SOUZA RODRIGUES**, portador(a) do **CPF nº 136.238.748-76**, vem, respeitosamente, à presença de Vossa Senhoria, com fundamento no **CREDENCIAMENTO nº 390004-01/2025**, estabelecido por meio da **Portaria SENATRAN nº 139, de 20 de fevereiro de 2025**, requerer:

1. Do Objeto do Pedido

Requerimento de complementação de documentos de habilitação para o Credenciamento nº 390004-01/2025, conforme Item 9.21.4 do Termo de Referência 116/2025 – Requisitos Técnicos.

Nestes termos,

Pede deferimento.

São Paulo, 06 de novembro de 2025.

Etelvina de Souza Rodrigues

ETELVINA DE SOUZA RODRIGUES
REPRESENTANTE LEGAL
JB3 SOFTWARES S.A.

Requerimento - Evidências .docx

Documento número #0a71dfdc-e3ec-474e-9fd8-ff3555454d34

Hash do documento original (SHA256): 23f55c80a9af108cf365d6c9d51b30372e4ac7f883f55d4a6176e8973f118eb5

Assinaturas

Etelvina de Souza Rodrigues

CPF: 136.238.748-76

Assinou em 06 nov 2025 às 14:46:02

Etelvina de Souza Rodrigues

Log

06 nov 2025, 14:43:15	Operador com email vina.rodrigues@jb3ti.com.br na Conta 364adf64-8a29-49c8-b03b-b471ecdbc9dc criou este documento número 0a71dfdc-e3ec-474e-9fd8-ff3555454d34. Data limite para assinatura do documento: 06 de dezembro de 2025 (14:43). Finalização automática após a última assinatura: habilitada. Idioma: Português brasileiro.
06 nov 2025, 14:44:54	Operador com email vina.rodrigues@jb3ti.com.br na Conta 364adf64-8a29-49c8-b03b-b471ecdbc9dc alterou o processo de assinatura. Data limite para assinatura do documento: 01 de janeiro de 2026 (17:19).
06 nov 2025, 14:44:54	Operador com email vina.rodrigues@jb3ti.com.br na Conta 364adf64-8a29-49c8-b03b-b471ecdbc9dc adicionou à Lista de Assinatura: vina.rodrigues@jb3ti.com.br para assinar, via E-mail. Pontos de autenticação: Token via E-mail; Nome Completo; CPF; Assinatura manuscrita. Dados informados pelo Operador para validação do signatário: nome completo Etelvina de Souza Rodrigues e CPF 136.238.748-76.
06 nov 2025, 14:46:02	Etelvina de Souza Rodrigues assinou. Pontos de autenticação: Token via E-mail vina.rodrigues@jb3ti.com.br. CPF informado: 136.238.748-76. Assinatura manuscrita com hash SHA256 prefixo cc62ba(...), vide anexo manuscript_12 ago 2025, 17-48-05.png. IP: 179.125.160.221. Localização compartilhada pelo dispositivo eletrônico: latitude -23.2587264 e longitude -46.6026496. URL para abrir a localização no mapa: https://app.clicksign.com/location. Componente de assinatura versão v1.1340.1 disponibilizado em https://app.clicksign.com.
06 nov 2025, 14:46:03	Processo de assinatura finalizado automaticamente. Motivo: finalização automática após a última assinatura habilitada. Processo de assinatura concluído para o documento número 0a71dfdc-e3ec-474e-9fd8-ff3555454d34.

Documento assinado com validade jurídica.
Para conferir a validade, acesse https://www.clicksign.com/validador e utilize a senha gerada pelos signatários ou envie este arquivo em PDF.
As assinaturas digitais e eletrônicas têm validade jurídica prevista na Medida Provisória nº. 2200-2 / 2001

Este Log é exclusivo e deve ser considerado parte do documento nº 0a71dfdc-e3ec-474e-9fd8-ff3555454d34, com os efeitos prescritos nos Termos de Uso da Clicksign, disponível em www.clicksign.com.

Anexos

Etelvina de Souza Rodrigues

Assinou o documento em 06 nov 2025 às 14:46:02

ASSINATURA MANUSCRITA
Assinatura manuscrita com hash SHA256 prefixo cc62ba(...)

Etelvina de Souza Rodrigues
manuscript_12 ago 2025, 17-48-05.png