PODER JUDICIÁRIO
TRIBUNAL DE JUSTIÇA
DO ESTADO DO AMAZONAS

Anna Leticia Pessoa de Brito Andrade <anna.brito@tjam.jus.br>

Itens 19 e 20 - Prova de conceito

2 mensagens

'Eduardo Fleischhauer - Br Supply' via Coordenação de Licitação <colic@tjam.jus.br> 9 de março de 2026 às 11:23
Responder a: Eduardo Fleischhauer - Br Supply <eduardo.f@brsupply.com.br>
Para: "colic@tjam.jus.br" <colic@tjam.jus.br>
Cc: licitacoes - BR Supply <licitacoes@brsupply.com.br>, Eduardo Fleischhauer - Br Supply <eduardo.f@brsupply.com.br>, "patrimonio@tjam.jus.br" <patrimonio@tjam.jus.br>

Prezados,

Cfe. alinhado, seguem os anexos.

Solicito confirmação de recebimento.

Att.

BrSUPPLY
Suprimentos Corporativos

Eduardo Fleischhauer
Gerente Executivo de Relacionamento Governamental - Inovação – Licitações – Compras Públicas
WhatsApp: 51 99388 4698
brsupply.com.br

Itens 19 e 20 - PCN e demais.zip
3289K

COLIC <colic@tjam.jus.br> 9 de março de 2026 às 11:24
Para: Eduardo Fleischhauer - Br Supply <eduardo.f@brsupply.com.br>
Cc: licitacoes - BR Supply <licitacoes@brsupply.com.br>, Eduardo Fleischhauer - Br Supply <eduardo.f@brsupply.com.br>, "patrimonio@tjam.jus.br" <patrimonio@tjam.jus.br>, Coordenação de Licitação <colic@tjam.jus.br>

Prezados,

Confirmamos o recebimento.

Atenciosamente,
[Texto das mensagens anteriores oculto]
--
Anna Letícia Pessoa de Brito Andrade
Membro da COLIC
SECOP/COLIC/TJAM

	Alta Disponibilidade Infraestrutura de TI	Versão: 4.1	Data: 27/01/2026
Autor: Fernando Gonçalves			
Revisor: Fernando Gonçalves			
Classificação da informação: Pública			

Alta Disponibilidade Infraestrutura de TI Br Supply

A Br Supply possui uma infraestrutura de alta disponibilidade, virtualizada, utilizando tecnologia VMware/PureStorage, utiliza contingência dos links de dados com a nuvem pública e na comunicação entre as demais unidades, há redundância dos firewalls e Hosts.

O Datacenter utiliza infraestrutura convergente replicada em dois pontos distintos de modo ativo, estão localizados no centro administrativo da Br Supply, na cidade de São Leopoldo-RS, na Avenida Presidente João Goulart, 401 e Rua Padre Réus, 48 - Bairro Padre Réus.

Utiliza proteção de acessos com firewalls de última geração Fortinet 200E, protege as aplicações WEB com firewall de nuvem WAF(FortiWAF) e protege a camada de DNS na TrustWave.

Tem como ferramenta de backup o software VEEAM com replicação do backup diário no CD de São Leopoldo.

Todos os equipamentos possuem garantia e suporte do fabricante até 2024.

Na estrutura de energia, possui nobreak com autonomia de 8h com processo de troca de baterias a bianual, conforme cronograma de manutenção dos equipamentos. E Gerador com autonomia de 10h sem abastecimento, podendo ser abastecido sem parada.

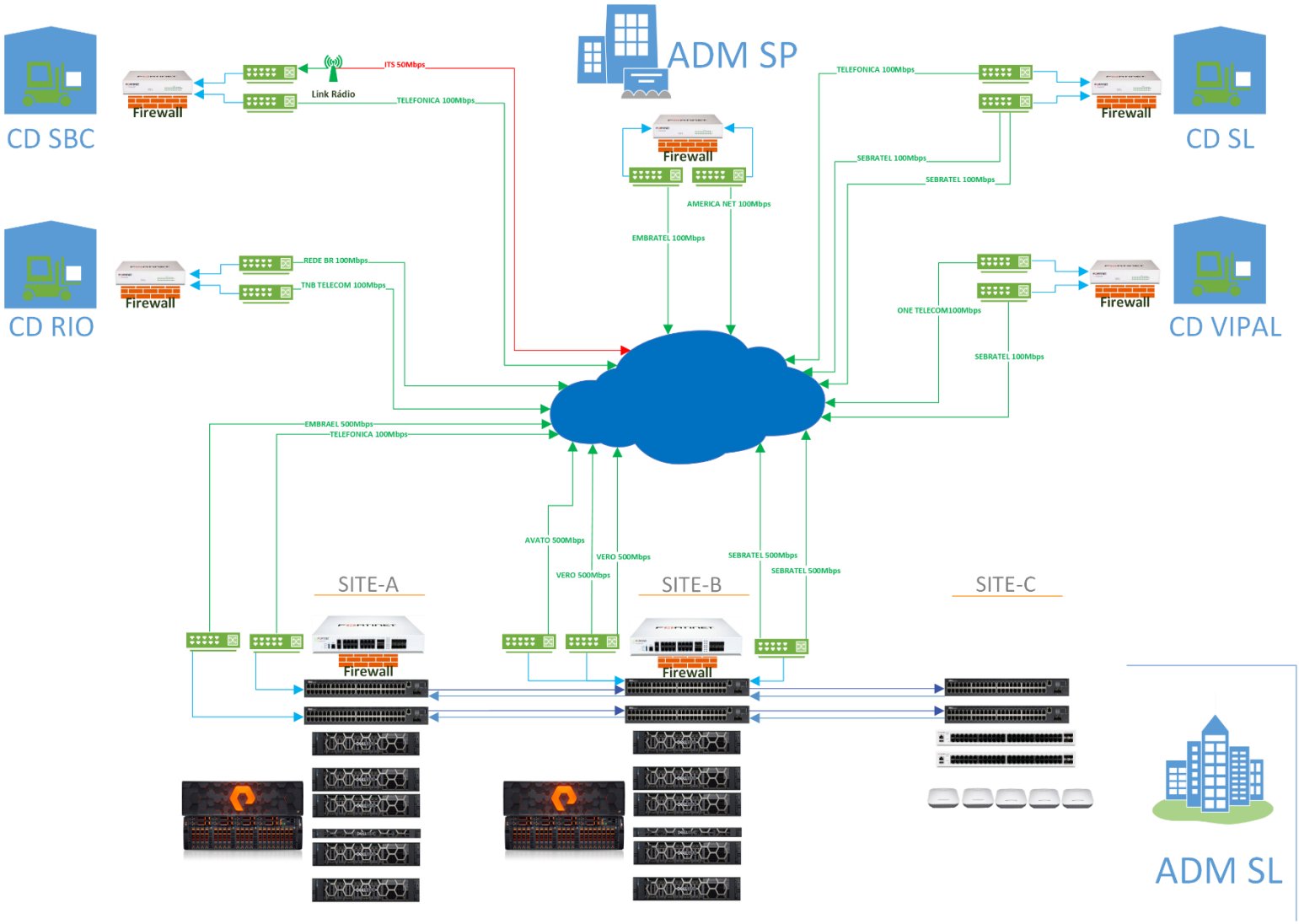
Este documento suporta o PRD definido no PCN.

BrSUPPLY Suprimentos Corporativos	Alta Disponibilidade Infraestrutura de TI	Versão: 4.1	Data: 27/01/2026
Autor: Fernando Gonçalves			
Revisor: Fernando Gonçalves			
Classificação da informação: Pública			

As informações contidas neste documento contemplam o ambiente de Infraestrutura da Br Supply.

1. **Comunicação entre redes (WAN)**

Está abaixo documentado a topologia de interligação entre as unidades da Br Supply.



2. Alta disponibilidade

A infraestrutura da Br Supply conta com Datacenter replicado entre dois sites distintos utilizando a tecnologia de virtualização VMware com Storage PureStorage, garantindo a alta disponibilidade de todos os serviços em casos de incidentes no ambiente físico.

3. Comunicação com a rede externa

Está abaixo documentado as conexões externas do datacenter da Br Supply.

3.1. Relação de links

Provedor	Serviço	Característica	Velocidade
VIVO	Internet	SD-WAN	500Mbps
VERO	Internet	SD-WAN	500Mbps
AVATO	Internet	SD-WAN	100Mbps
Claro	Internet	SD-WAN	500Mbps

4. Servidores DNS Externos

A zona de DNS da Br Supply está armazenada no fornecedor TrustWave para a devida utilização da ferramenta de WAF (Web Application Firewall) que atua sobre as aplicações WEB.

O gerenciamento dessa camada é efetuado somente pelo suporte da Gruppen.

5. Segurança na comunicação entre redes (Firewall)

Está abaixo documentado o ambiente Firewall.

5.1. Relação de Firewalls

Equipamento/Servidor	Hardware	IP
Fortinet	201F	192.168.0.1
Fortinet - HA	201F	192.168.0.1

6. Acesso ao Data Center

Os servidores estão alocados no Data Center da Br Supply em local fechado. O acesso ao Data Center é feito através de chave. O acesso aos servidores deve ser solicitado a equipe de Infraestrutura da Br Supply.

O Data Center possui climatização adequada e termômetro para medição de umidade e temperatura e forma externa.

7. Área de armazenamento de dados em rede (Storage)

Possui storage de última geração **PureStorage** com discos flash NVMe.

Possui storage para armazenamento dos dados de backup QNAP TS 431P, que possibilita o restore rápidos dos dados.

7.1. Processo de restabelecimento do serviço

O serviço de armazenamento possui redundância ou contingência. A equipe de Infraestrutura presta suporte ao serviço de armazenamento que é encarregada do restabelecimento.

8. Segurança de endpoint (Antivírus-EDR-XDR)

É utilizada a ferramenta de XDR SentinelOne. E é de responsabilidade da equipe de Infraestrutura da Br Supply, configuração, instalação de agentes, varredura e verificação dos relatórios gerados na ferramenta, conta com recurso de IA para análise de ameaças em tempo real.

9. Publicação ServiçosWEB (IIS)

Os serviços WEB publicados pela Br Supply estão protegidos por WAF (Web Application Firewall) fornecido pela empresa Fortinet - FortiWeb.

O serviço é gerenciado pela Gruppen empresa especializada e certificada no portifólio de segurança da Fortinet.

9.1. Abaixo relação de serviços web publicados.

Serviço	Servidor	IP Externo	IP Interno
ftp.brsupply.com.br	[redacted]	[redacted]	[redacted]
adfs.brsupply.com.br	[redacted]	[redacted]	[redacted]
brsupply.com.br	[redacted]	[redacted]	[redacted]

wbsvc.brsupply.com.br	[redacted]	[redacted]	[redacted]
supplymanager.com.br	[redacted]	[redacted]	[redacted]
punchout.brsupply.com.br	[redacted]	[redacted]	[redacted]

10. Relação de gateways de navegação

O gateway default da rede de computadores da Br Supply é o firewall de perímetro da rede.

10.1. Abaixo relação de equipamento

Equipamento/Servidor	Hardware	Sistema Operacional
Fortinet - Fortigate	201F	NA
Fortinet - Fortigate	201F - HA	NA

10.2. Modalidade de Suporte

O suporte ao serviço, política de controle de navegação e filtros de conteúdo – Fortigate é de responsabilidade da equipe de Infraestrutura da Br Supply, configuração de regras e liberação de acessos.

10.3. Processo de restabelecimento do serviço

O processo de navegação e filtro de conteúdo – Fortigate possui redundância, os firewalls estão configurados em HA.

11. Backup e recuperação de dados (Backup/Restore)

O backup é gerenciado pela ferramenta VEEAM executado diariamente com replicação no CD de São Leopoldo o backup dos bancos de dados é efetuado de hora em hora.

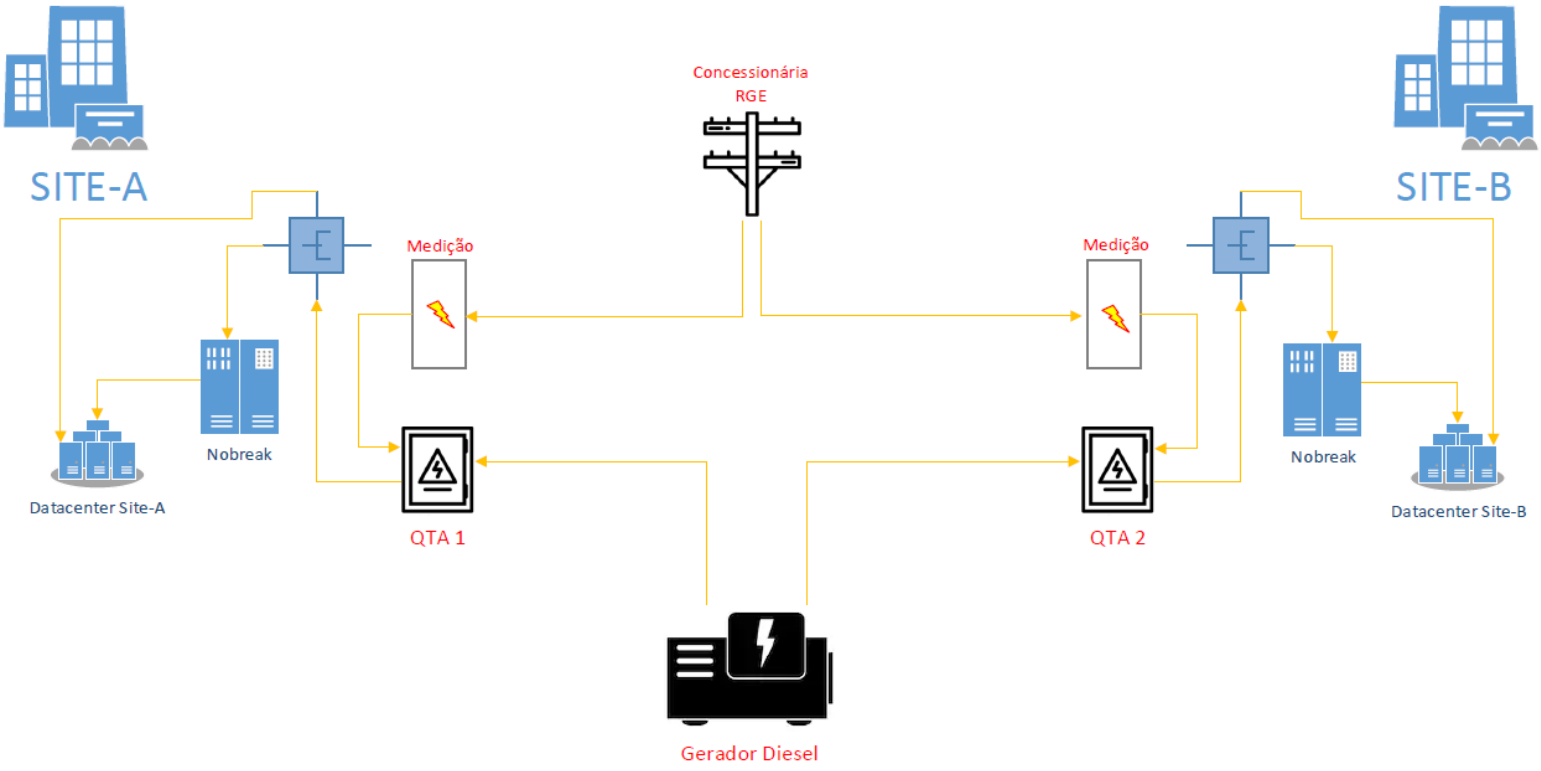
11.1. Relação de servidores de Backup

Servidores	Tecnologia	Sistema Operacional	IP
SRVVEEAM011	VEAAM	[redacted]	[redacted]

11.2. A restauração de dados pode ser feita a qualquer momento no ambiente atual ou em qualquer outro ambiente estruturado com a tecnologia de virtualização VMware.

12. Contingência de energia

A Br Supply possui nobreak com autonomia de 8h, (a troca de baterias é feita bienalmente conforme cronograma de manutenção dos equipamentos), as unidades possuem gerador a diesel, com tanque para autonomia de 10h e capacidade de reabastecimento sem parada, o gerenciamento dos equipamentos e feito pela infraestrutura da Br Supply.



13. Telefonia

Está abaixo documentado o ambiente de telefonia.

13.1. Relação de servidores e equipamentos de telefonia

Servidor PABX Net2phone	IP
PABX em nuvem VIVO VVN	[redacted]

13.2. Acesso ao hardware

O PABX de telefonia está localizado no Data Center tier 3 da VIVO de modo replicado.

14. Suporte Especializado

A Br Supply conta com contrato de suporte técnico com a empresa Gruppen.

14.1. Modalidade de suporte

Engloba toda a infraestrutura da Br Supply.

Suporte 24X7 para todos os equipamentos, rede, sistemas operacionais, Sistemas de virtualização, firewalls, ferramentas de segurança tais como endpoints e banco de dados SQL.

Possui serviço de SIEM contratado para monitoramento do domínio e endereços core da rede.

O atendimento é feito em tempo real através do telefone de suporte telefônico - 3079-1100 ou e-mail: suporte@gruppen.com.br.

Anonimização, Bloqueio e Exclusão de Dados	Versão: 2.0	Data: 04/11/2024
Autor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Revisor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Classificação da informação: Pública		

CRITÉRIOS PARA ANONIMIZAÇÃO, BLOQUEIO E EXCLUSÃO DE DADOS PESSOAIS

BRS SUPRIMENTOS CORPORATIVOS S/A

1. ANONIMIZAÇÃO

1.1. Conceito

A anonimização consiste no processamento de dados pessoais para remover ou modificar informações que possam identificar um indivíduo, conforme art. 5º, inciso III, da Lei nº 13.709/2018 (LGPD). Dados anonimizados não podem ser associados a indivíduos específicos por meio de esforços razoáveis.

1.2. Finalidade

A anonimização protege a privacidade dos titulares ao:

- Restringir o acesso a informações por pessoas não autorizadas.
- Reduzir os riscos em casos de incidentes de segurança.

1.3. Critérios

Os critérios para anonimização incluem:

- Impossibilidade de identificação direta ou indireta do titular.
- Uso de métodos técnicos robustos, irreversíveis por meios razoáveis.
- Avaliação periódica da eficácia da técnica empregada.

1.4. Técnicas

A equipe de Tecnologia da Informação é responsável por definir as técnicas de anonimização, assegurando sua eficácia. Métodos podem incluir:

- Generalização de dados.
- Supressão de atributos identificáveis.
- Perturbação de dados (noise addition).

1.5. Aplicação

Os dados pessoais tratados incluem informações de colaboradores, clientes, candidatos e fornecedores, como nome, CPF, endereço e informações bancárias. O processo de anonimização será gerenciado pelo setor de TI e aplicado conforme a necessidade operacional.

2. BLOQUEIO DE DADOS PESSOAIS

2.1. Conceito

O bloqueio de dados, conforme art. 5º, inciso XIII, da LGPD, refere-se à suspensão temporária do tratamento de dados, mantendo-os armazenados de forma segura.

2.2. Finalidade

Permitir a restrição temporária ou circunstancial do tratamento de dados, conforme solicitação do titular ou necessidade operacional.

2.3. Critérios

- Dados bloqueados não podem ser tratados até nova autorização do titular.
- Manutenção de registros bloqueados para atender obrigações legais ou

regulatórias.

2.4. Aplicação

- Dados de colaboradores: documentos de identificação, contratos e comprovantes salariais devem ser mantidos conforme legislação aplicável (ex.: 5 anos para dados trabalhistas).
- Dados de clientes e fornecedores: bloqueio será definido pelo Comitê de Proteção de Dados em prazo apropriado.

3. EXCLUSÃO DE DADOS PESSOAIS

3.1. Conceito

A exclusão de dados pessoais é a eliminação definitiva de registros, tornando-os irrecuperáveis, conforme art. 5º, inciso XIV, da LGPD.

3.2. Finalidade

- Garantir o direito do titular à eliminação de seus dados.
- Minimizar riscos relacionados ao armazenamento excessivo.

3.3. Critérios

- A exclusão deve ser definitiva e irreversível.
- Métodos de exclusão incluem:
    - Dados digitais: remoção segura com uso de ferramentas especializadas.
    - Dados físicos: destruição por trituradores e descarte seguro.

3.4. Prazos

Os prazos para retenção e exclusão de dados respeitarão legislações aplicáveis:

- Dados trabalhistas: 5 anos (Constituição Federal).
- Encargos sociais: até 30 anos (ex.: FGTS, INSS).
- Dados de clientes: exclusão periódica, conforme política interna.

4. RESPONSABILIDADES E CONTROLES

- A equipe de TI e o Comitê de Proteção de Dados serão responsáveis por:
    - Garantir a implementação de medidas adequadas.
    - Avaliar e revisar processos periodicamente.
- Contratos com terceiros incluirão cláusulas de conformidade com a LGPD.

5. DISPOSIÇÕES FINAIS

Esta política será revisada regularmente para assegurar conformidade com a LGPD e boas práticas de proteção de dados. Dúvidas ou solicitações devem ser direcionadas ao Comitê de Proteção de Dados.

Manual de Registro de Incidentes	Versão: 1.0	Data: 02/07/2021
Autor: Russell Bedford Brasil		
Revisor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Classificação da informação: Pública		

POLÍTICA DE REGISTRO DE INCIDENTES DA

BRS SUPRIMENTOS CORPORATIVOS

1. OBJETIVO

Definir regras e procedimentos de segurança para o registro de ocorrência de incidentes no ambiente de tecnologia e/ou analógico utilizado pela BRS SUPRIMENTOS CORPORATIVOS, em conformidade com o art. 48 da Lei nº 13.709/2018 (LGPD).

2. ABRANGÊNCIA

Este regulamento se aplica a todo o tratamento de dados pessoais realizados na BRS SUPRIMENTOS CORPORATIVOS.

Este regulamento está alinhado com a Política de Segurança da Informação, Cartilha TI, Política de Acesso, Plano de Alta Disponibilidade e Infraestrutura da TI. da BRS SUPRIMENTOS CORPORATIVOS

3. IMPLEMENTAÇÃO

O departamento responsável pela Segurança da Informação e as chefias das áreas da empresa desenvolverão as ações necessárias e contínuas para implementação do regulamento, ficando o departamento de TI responsável pela coordenação das ações de tecnologia e, o departamento de estratégia por atitudes referentes aos incidentes analógicos.

4. REGRAS E PROCEDIMENTOS

4.1. Ocorrência de incidente

Todo incidente envolvendo dados pessoais que possa acarretar risco ou dano

relevante aos titulares de dados deve ser registrado pelos colaboradores e comunicado às equipes de Tecnologia da Informação e ao departamento de Estratégia, que adotarão os procedimentos necessários.

4.2. Tratamento da ocorrência do incidente

A equipe do setor de Tecnologia da Informação ou o setor de Estratégia deve:

a) Registrar o incidente nos sistemas da empresa.
b) Comunicar à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares de dados sobre o incidente e os possíveis riscos e/ou danos.
c) A comunicação deverá ser realizada em prazo razoável e deverá mencionar, no mínimo:
    - Descrição da natureza dos dados pessoais afetados;
    - As informações sobre os titulares envolvidos;
    - Indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;
    - Os riscos relacionados ao incidente;
    - Os motivos da demora, no caso de a comunicação não ter sido imediata;
    - As medidas que foram ou serão adotadas para reverter ou mitigar os efeitos do prejuízo.
d) Acompanhar as ações desenvolvidas para solução definitiva da causa do incidente.
e) Avaliar a necessidade de criação de novos mecanismos de controle de segurança da informação, com objetivo de evitar novos incidentes.
f) Emitir relatório gerencial sobre o incidente ocorrido, indicando a solução encontrada para o caso, as medidas adotadas para minimização dos danos e as providências definidas pela ANPD.

4.3. Tratamento após a solução definitiva do incidente

A BRS SUPRIMENTOS CORPORATIVOS deverá fazer o gerenciamento de causas mais frequentes, tipos de incidentes e áreas nas quais ocorreram, com intuito de fazer a gestão efetiva para identificar problemas que podem gerar incidentes e solucionar as questões.

5. CONTROLES E RESPONSABILIDADES

As equipes de Tecnologia da Informação e setor de Estratégia, também responsáveis pela Segurança da Informação, deverão manter este manual atualizado e, se necessário, gerar outros documentos relativos aos procedimentos para o controle do acesso remoto pelo usuário ou para utilização de documentos físicos fora das dependências da empresa.

6. CONCLUSÃO

O descumprimento deste manual e/ou dos demais instrumentos normativos que complementam o processo de segurança da informação constitui falta grave, passível de penalidades administrativas e contratuais.

Situações de excepcionalidade não previstas deverão ser definidas pelas equipes de Tecnologia da Informação e outros setores responsáveis, com apoio da gestão, considerando as áreas da organização que estejam envolvidas.

Plano de Continuidade de Negócio

V1R2

Objetivos do Plano

Definir as ações aplicáveis com base na estrutura da Br Supply e assegurar que todos conheçam o Plano de Continuidade de Negócio (PCN)

A Br Supply possui um Plano de Continuidade de Negócios corporativo, suportado por uma infraestrutura de alta disponibilidade ativa-ativa, garantindo a continuidade dos processos críticos do negócio.

Processos Vitais

• Recebimento de pedidos (Administrativo)
• Liberação de pedidos (Administrativo)
• Separação (Operação CD)
• Embarque (Operação CD)
• Entrega (Operação CD)

Premissas e Objetivos do Projeto

O Plano de Continuidade de Negócios (PCN) assegura à Br Supply a continuidade de seus negócios em caso de paralisação, decorrente de sinistro, de um ou mais processos considerados críticos. O sinistro torna-se realidade quando ameaças internas ou externas exploram as vulnerabilidades dos processos. Os processos críticos ao negócio foram mapeados por meio de levantamento de informações com os Gestores das principais áreas de negócio. Para tanto, o PCN é definido como (PCN = PAC + PCO + PRD), a saber:

• PAC - Programa de Administração da Crise – É acionado após decretada a Crise, e é voltado para todo o processo. Tem seu término quando se volta à normalidade;
• PCO - Plano de Continuidade Operacional – São acionados os primeiros procedimentos do PAC, e é voltado aos processos de negócio;
• PRD - Plano de Recuperação de Desastres – É acionado junto com o PCO, e é focado na recuperação/restauração de componentes que suportam o PCN.

O desenvolvimento do Plano de Continuidade de Negócios é baseado na avaliação dos processos críticos estabelecidos pela Administração compreendendo às suas principais etapas:

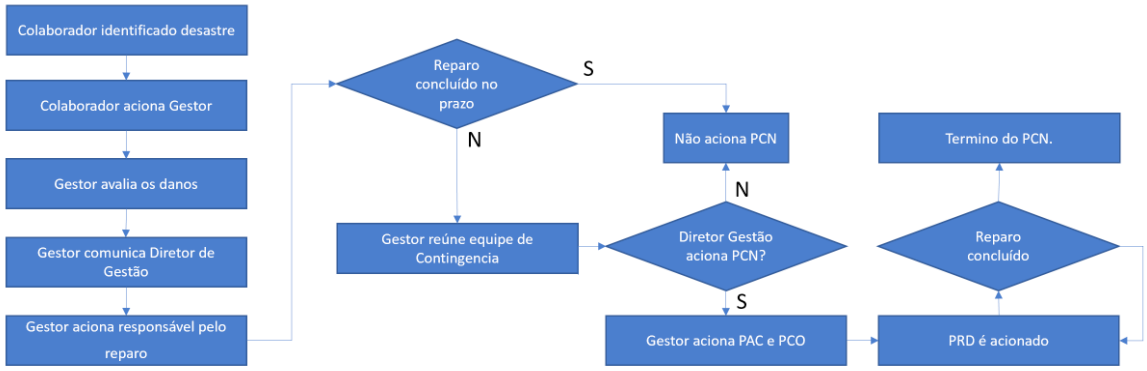
• Análise de riscos de TI;

• Análise de Impacto nos Negócios (BIA);

• Estratégia de recuperação.

A manutenção do PCN atualizado e o treinamento dos colaboradores são fatores crítico de sucesso.

Diagrama geral do PCN Br Supply



Site Principal e Site de Contingência

A Br Supply possui cinco unidades operacionais sendo: três em São Leopoldo / RS, uma em São Paulo / SP e uma em São Bernardo do Campo / SP.

Em operação normal, os processos Administrativos/Comerciais são efetuados nas sedes administrativas denominadas Site A, Site B, Site C e ADM SP respectivamente, enquanto os processos de operação de CD ocorrem nos CDs SL e CD SBC, contado com HUBs de apoio no RJ, MG, DF e ES.

As unidades de contingência contêm os mesmos recursos tecnológicos da unidade principal, podendo cada estação de trabalho utilizar tanto a unidade principal como o de contingência. Os sistemas de gestão de pedidos e atendimento (Supply Manager, E-mails, relatórios e controles de gestão) são web. Os telefones podem ser migrados para outra central telefônica. Portanto, em situações de contingência, os funcionários são designados pelo Diretor de Gestão a se dirigir para o(s) endereço(s) alternativo(s), ou a transferir a operação para a equipe deste local, de forma que haja o mínimo de impacto possível dentro das atividades da empresa.

Mapeamento e relacionamento de contingência dos sites:

Administrativo / Comercial Sul		
Principal	**Contingência 1**	**Contingência 2**
Site A Rua Pres. João Goulart, 401 São Leopoldo / RS	Site B Rua Padre Réus, 48 São Leopoldo / RS	Site C Rua do Parque, 11 São Leopoldo / RS

CD Sul	
Principal	**Contingência**
CD SL Av. Parobé, 4851 – RS240 São Leopoldo / RS	CD SBC R. José Martins Fernandes, 601, G32 São Bernardo do Campo – SP

Administrativo / Comercial São Paulo	
Principal	**Contingência**
ADM SP Av. Francisco Matarazzo, 1500 - 9º Andar São Paulo / SP	CD SBC R. José Martins Fernandes, 601, G32 São Bernardo do Campo – SP

CD SP	
Principal	**Contingência**
CD SBC R. José Martins Fernandes, 601, G32 São Bernardo do Campo – SP	CD SL Av. Parobé, 4851 – RS240 São Leopoldo / RS

Processos e Sistemas Críticos

Processo crítico pode ser definido como um processo de trabalho que, uma vez paralisado por tempo superior ao definido pela unidade gestora do negócio, irá afetar sensivelmente as operações e serviços da organização gerando maior impacto nos clientes internos e externos, definido pela fórmula (MTD = RTO + WRT).

Definição:

• MTD (Maximum Tolerable Downtime): é o tempo máximo que um processo negócio pode tolerar indisponível. Diferentes processos de negócio terão diferentes MTD's.
• RTO (Recovery Time Objective): é a meta de tempo para recuperar sistemas e recursos após uma indisponibilidade.
• WRT (Work Recovery Time): é o tempo para restaurar os sistemas (hardware, software e configuração) das funções de negócios críticas.

1. Processos com MTD de 15 minutos no período entre 8h e 18h

Área	Processo	Sistema
Administrativo / Comercial	Recebimento de pedidos	Supply Manager

2. Processos com MTD de 5 horas no período entre 8h e 18h

Área	Processo	Sistema
Administrativo / Comercial	Liberação de pedidos	Supply Manager

3. Processos com MTD de 4 horas no período entre 7h e 22h

Área	Processo	Sistema
Operação CD	Separação	WMS
Operação CD	Embarque	SAP
Operação CD	Entrega	Supply Manager

Abrangências

Ameaças Relacionadas
No entendimento dos gestores das áreas avaliadas as ameaças com grau de vulnerabilidade significante estão divididas em:

a. **Humanas:** Greves, Distúrbio Civil, Falha de Prestador de Serviços/Parceiro, Acesso Indevido às Instalações e Erro Humano não intencional.
b. **Tecnológicas:** Falha em Aplicativo (SW), Falha em Hardware (HW), Falha em sistemas Operacionais, Vírus de Computador, Falha em Rede Interna (LAN), Falha na Entrada de Dados, Falha em Rede Externa (WAN), Falha de Telecom – Dados e Falha em Sistema de Acesso.
c. **Infraestrutura:** Falha em Telecom - Voz, Falha em Sistema de Refrigeração, Interrupção de Energia Elétrica, Falha em Instalações Elétricas.
d. **Naturais:** Alagamento Interno do Ambiente, Queda de Raios, Vendaval e Incêndio. e. Físicas Problema Estrutural ou de Instalações e Rompimento de Tubulação Interna (água, esgoto e gás).

Cabe ressaltar que paradas não programadas podem resultar em perdas tangíveis e intangíveis, acarretando perda de confiança de colaboradores e clientes nos processos de negócios. Desta forma, os potenciais impactos apontados pelos gestores numa eventual interrupção são:

• Interrupção de prestação de serviços a clientes;
• Multas e sanções;
• Perda da capacidade de gestão e controle;
• Comprometimento da imagem da organização;
• Exposição negativa na mídia e perda de vantagem competitiva.

Ações e Procedimentos

Todos os colaboradores estão aptos a identificar as ameaças que possam levar a paralisação dos negócios e comunicar imediatamente ao Gestor.

ADMINISTRAÇÃO COMERCIAL E OPERAÇÃO INTRALOGÍSTICA

Impossibilidade de acesso ao prédio ou deslocamento dos funcionários, dentre as quais destacamos:

• Princípio de Incêndio;
• Ameaça de Bomba;
• Bloqueios;
• Manifestações;
• Desastres Naturais;

Ações:
-Até10 minutos após a evidência, Gestor entrará em contato com a Administração de Patrimônio para esclarecimentos e caso necessário, também fazer contato com os seguintes órgãos públicos: Bombeiros: 193 (Incêndio e Ameaça de Bomba); Defesa Civil: 199 (Ameaça de Bomba, Greves, Bloqueios e Inundações); Polícia Civil: 147 (Ameaça de Bomba, Roubo e Furto de Informações e ativos).

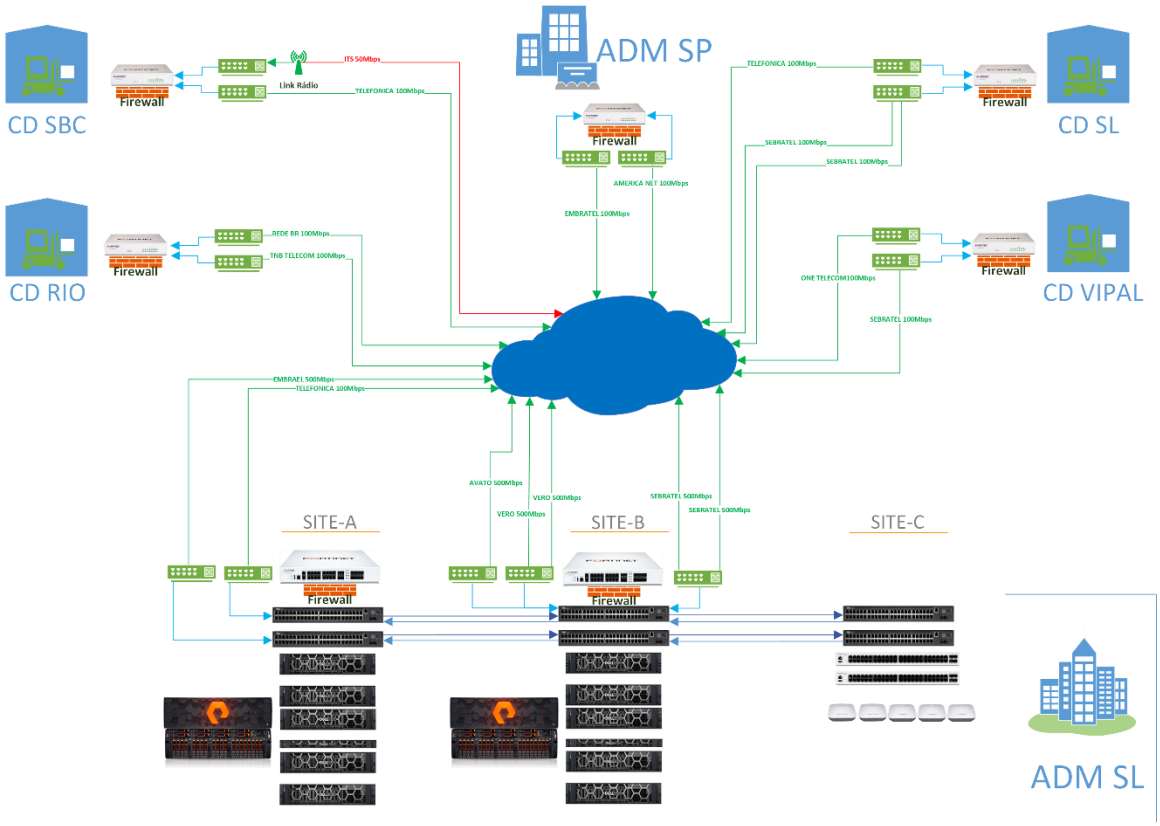
-Até 20 minutos após a conclusão da etapa anterior, o gestor deve entrar em contato com o Diretor de Gestão, que definirá os colaboradores que atuarão no site de contingência, bem como avisar os componentes que atuarão em regime Home Office. Avisar aos integrantes das áreas contingenciadas para que se dirijam ao endereço do site redundância, direcionando os telefones para o site de contingência para sequência no atendimento, ou em último caso, para as residências para atuação no regime Home Office, conforme relação indicada abaixo:

Área Contingenciada	Nome	Contato	E-mail
Patrimônio	Rodrigo Ivo	(51)982348059	rodrigo.pereira@brsupply.com.br
Administrativo	Dalton Schmitt	(51)991286806	dalton.schmitt@brsupply.com.br
Comercial	Eliandro Arena	(51)992496190	eliandro.arena@brsupply.com.br
Operações	Bruno Soares	(51)991217210	bruno.soares@brsupply.com.br
TI – Sistemas	Alexandre Cembranel	(51)999641633	alexandro.cembranel@brsupply.com.br
TI - Infraestrutura	Fernando Gonçalves	(51)999617127	fernando.goncalves@brsupply.com.br

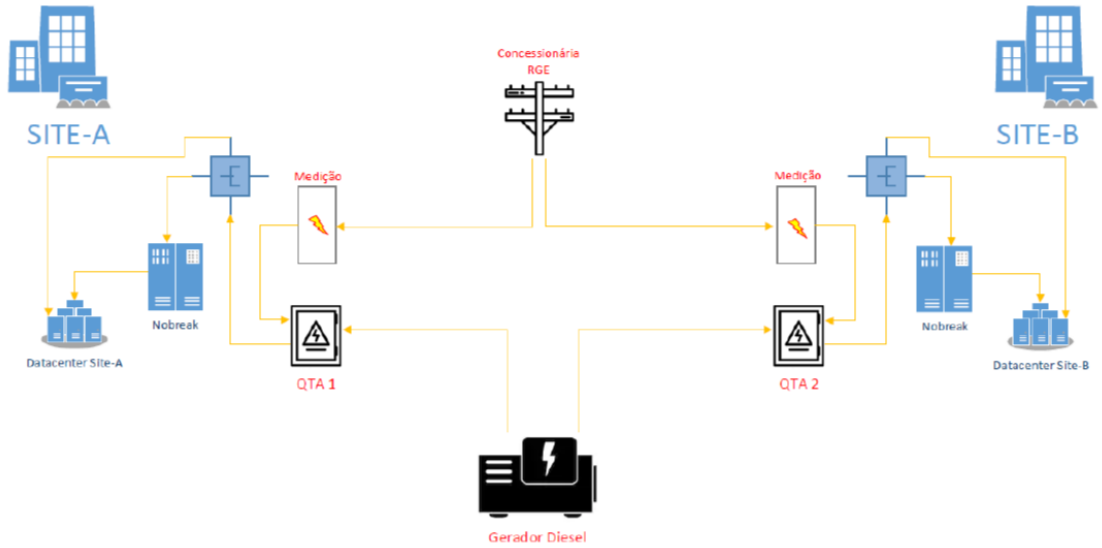
INFRAESTRUTURA E TECNOLOGIA

As quedas de sistemas, links e infraestrutura de servidores, identificadas pelo monitoramento ativo reportam os incidentes ao Gestor de Infraestrutura. O Gestor de Infraestrutura efetua a confirmação de efetividade da contingência e, em até 10 minutos após a evidência aciona as equipes (contratos de suporte) para atendimento e solução. Em caso de inoperância também da contingência, em até 20 minutos após a conclusão da etapa anterior, o gestor deve entrar em contato com o Diretor de Gestão para acionamento da equipe que fara a restauração do backup, as devidas comunicações e operações em contingência.

Estrutura de redundância de sistemas:



Estrutura de redundância de alimentação



PROCEDIMENTOS DE RETORNO À NORMALIDADE

Cabe ao Diretor de Gestão encerrar o PCN e comunicar aos Gestores envolvidos no processo. Quando o acesso ao prédio estiver liberado e em condições de normalidade, comunicar a todos os colaboradores por meio de seus gestores para que retornem aos seus postos de trabalho.

Administração do Plano

A continuidade de negócios de uma organização, assim como a recuperação de desastres é o resultado da execução e da manutenção de um processo contínuo que envolve planejamento, formalização, monitoração e melhorias. O processo de Continuidade de Negócios é de responsabilidade e gestão da área de Controladoria, que determina o ciclo e as etapas que deverão ser executadas para que tanto os cenários de risco e impacto sobre os negócios como as estruturas e estratégias que embasam o PCN possam ser atualizadas refletindo o ambiente de negócios da empresa. Para que a área de TI possa verificar o grau de atualização do PCN e decidir quanto ao momento em que o processo de continuidade de negócios será atualizado,

os processos de planejamento de negócios e tecnológico, gerenciamento de mudanças, gerenciamento de riscos, tratamento de problemas e de incidentes devem prever a participação desta área nas decisões relevantes destes processos.

Divulgação e Treinamento

Os fatores críticos de sucesso deste plano são o conhecimento e a familiaridade das pessoas e demais envolvidos na execução das atividades de continuidade de negócios e recuperação de desastres com as estratégias e recursos definidos no planejamento. Para que seja possível esta familiaridade e conhecimento do plano, conferindo-lhe credibilidade, a direção definiu que serão realizadas anualmente sessões de divulgação a todos os colaboradores e envolvidos no planejamento de continuidade de negócios. Estas sessões serão organizadas pela área de TI em conjunto com a área de Controladoria com o objetivo de manter os colaboradores atualizados sobre os conceitos de continuidade adotados, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação de desastres e continuidade de negócios.

Realização de Testes

Os testes têm por objetivo assegurar a eficiência e a efetividade do PCN e deverão ser planejados e executados com periodicidade mínima anual a partir da data da sua implantação. A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da área de Tecnologia da Informação. Os cenários deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela alta administração, que dever ser arquivado por um período mínimo de 5 (cinco) anos. Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nos ambientes de negócios da empresa e deverão ser conduzidos pela equipe de contingência em total conformidade com o definido. As simulações deverão ser realizadas sobre cenários e ameaças contemplados no plano, devendo cobrir os riscos e ameaças com maior probabilidade de ocorrência.

Controle de Versão

Versão	Data	Nome	Ação	Conteúdo
V1R0	01/06/2019	FG	Elaboração	Primeira versão do documento
V1R1	06/01/2020	JS	Atualização	Atualização gestores
V1R2	05/02/2026	FG	Atualização	Atualização de dados

Política de Classificação da Informação	Versão: 2.0	Data: 04/11/2024
Autor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Revisor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Classificação da informação: Pública		

POLÍTICA DE CLASSIFICAÇÃO DA INFORMAÇÃO

BRS SUPRIMENTOS CORPORATIVOS S/A

1. DIRETRIZES GERAIS

Esta política integra a Política de Segurança da Informação da BRS SUPRIMENTOS CORPORATIVOS, sendo aplicável a todos os funcionários, fornecedores, prestadores de serviços e terceiros vinculados à empresa.

A classificação da informação segue as diretrizes estabelecidas no Anexo A.8.2 da norma ISO/IEC 27001, assegurando que informações recebam o nível de proteção adequado, de acordo com sua importância e sensibilidade.

Definições:

- Informação: Dados ou representações significativas, independentemente do suporte ou forma de veiculação.
- Segurança da Informação: Proteção contra ameaças para garantir continuidade do negócio, minimizando riscos e maximizando eficiência.
- Confidencialidade: Garantia de que informações sejam acessadas somente por pessoas ou processos autorizados.
- Gestor da Informação: Responsável pela classificação e gestão das informações em sua área de competência.
- Rótulo: Identificação clara da classificação da informação.

2. CLASSIFICAÇÃO DAS INFORMAÇÕES

As informações da BRS SUPRIMENTOS CORPORATIVOS são classificadas nos seguintes níveis de confidencialidade:

1. Pública: Acesso irrestrito, podendo ser compartilhada com qualquer pessoa sem prejuízo. Exemplos: materiais de marketing, comunicados oficiais.
2. Interna: Restrita a funcionários e prestadores de serviços. Vazamentos

podem causar prejuízos moderados.

3. Secreta: Acesso limitado à área envolvida (ex.: Comercial, Financeiro). Vazamentos podem gerar perdas significativas (financeiras ou reputacionais). Controle rigoroso e descarte seguro são obrigatórios.

4. Sigilosa: Informações protegidas por legislações específicas (ex.: fiscais, bancárias). Acesso restrito à Diretoria e profissionais autorizados. O tratamento deve obedecer a normas específicas e controles rigorosos.

Prazo de Restrição:

- Interna: 2 anos
- Secreta: 5 anos
- Sigilosa: Conforme legislação específica ou 5 anos, o que for maior.

Após o prazo de restrição, a informação será automaticamente reclassificada como pública, salvo especificação em contrário.

3. RESPONSABILIDADES

3.1. Competência para Classificação:

- O gestor da informação é responsável por classificá-la e garantir sua proteção.
- Em caso de dúvidas, a Diretoria define a classificação adequada.

3.2. Reclassificação:

- Informações podem ser reclassificadas a qualquer momento pelo gestor ou mediante solicitação fundamentada.

4. PROCEDIMENTOS DE CLASSIFICAÇÃO

Todas as informações não públicas devem ser acompanhadas de documentação que contenha:

- Grau de confidencialidade;
- Grupos autorizados a acessar;
- Assunto;
- Fundamento da classificação;
- Prazo de restrição ou termo final;
- Identificação do responsável.

As informações devem ser classificadas no momento de sua criação ou recebimento, com histórico mantido em caso de alterações.

5. ROTULAÇÃO

- A rotulação é obrigatória para informações Internas, Secretas e Sigilosas, incluindo:
    - Grau de confidencialidade;
    - Grupos autorizados;
    - Prazo de restrição ou termo final.
- Para informações Públicas, a rotulação é opcional.

6. CONTROLES E PROTEÇÃO

- O acesso e tratamento de informações seguem o princípio do "necessário para saber".
- Contratos com terceiros devem incluir cláusulas de confidencialidade.
- Controles administrativos e tecnológicos serão definidos conforme o nível de confidencialidade e impacto potencial de vazamentos.

7. DISPOSIÇÕES FINAIS

Esta política será revisada periodicamente para assegurar sua aderência a legislações e boas práticas de mercado. Quaisquer dúvidas ou solicitações relacionadas à classificação de informações devem ser encaminhadas à área de Segurança da Informação.

Política de Gestão de Riscos	Versão: 2.0	Data: 21/08/2025
Autor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Revisor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Classificação da informação: Pública		

POLÍTICA DE GESTÃO DE RISCOS

BRS SUPRIMENTOS CORPORATIVOS S/A

1. INTRODUÇÃO

A BRS SUPRIMENTOS CORPORATIVOS estabelece, por meio da presente Política de Gestão de Riscos, os princípios e diretrizes de gestão dos riscos corporativos.

Esta Política também contempla os riscos relacionados ao tratamento de dados pessoais, em conformidade com a Lei Geral de Proteção de Dados (Lei nº 13.709/2018 – LGPD), buscando assegurar que as práticas corporativas estejam alinhadas à legislação e aos direitos fundamentais de privacidade e proteção de dados.

2. OBJETIVOS

A Política de Gestão de Riscos da BRS SUPRIMENTOS CORPORATIVOS tem por finalidade desenvolver, disseminar e implementar metodologias de gerenciamento de riscos corporativos e controles internos, com vistas a apoiar melhorias contínuas nos processos organizacionais, projetos e iniciativas estratégicas da BRS SUPRIMENTOS CORPORATIVOS, contribuindo para o alcance dos objetivos estratégicos e cumprimento do propósito institucional.

Adicionalmente, visa assegurar que os riscos associados ao tratamento de dados pessoais sejam identificados, avaliados e tratados adequadamente, em linha com a LGPD e demais regulamentações aplicáveis.

3. DIRETRIZES GERAIS

A Gestão de Riscos da BRS SUPRIMENTOS CORPORATIVOS foi implementada, observando as seguintes diretrizes:

➢ Colaborar para a consecução do propósito, visão e objetivos estratégicos da BRS SUPRIMENTOS CORPORATIVOS;

➢ Salvaguardar os interesses, reputação, marca e atividades da empresa;

➢ Proteger o ambiente interno da organização;

➢ Melhorar processos organizacionais;

➢ Subsidiar a tomada de decisões conscientes;

➢ Ser sistemática e estruturada;

➢ Considerar fatores humanos e culturais;

➢ Respeitar todos os colaboradores e stakeholders;

➢ Ser transparente e inclusiva;

➢ Ser dinâmica, interativa e capaz de reagir a mudanças;

➢ Aderir à integridade e aos valores éticos;

➢ Garantir a confidencialidade, integridade e disponibilidade de dados pessoais;

➢ Tratar dados pessoais somente para finalidades legítimas, específicas e informadas;

➢ Respeitar os direitos dos titulares de dados;

➢ Promover a cultura de proteção de dados entre colaboradores e parceiros.

4. GESTÃO DOS RISCOS

A Gestão de Riscos visa a auxiliar nas melhorias contínuas dos processos organizacionais, projetos e iniciativas estratégicas no âmbito da BRS SUPRIMENTOS CORPORATIVOS, provendo segurança para o cumprimento do propósito e do alcance dos objetivos organizacionais.

Para isso, a operacionalização da Gestão de Riscos observa, no mínimo, os seguintes requisitos:

➢ Criação do ambiente interno: conjunto de atitudes que caracterizam a forma como a organização define e trata os riscos.

➢ Definição de objetivos alinhados ao propósito e à visão da empresa.

➢ Identificação de eventos de risco: incluindo incidentes de segurança da informação e violações de dados pessoais.

➢ Avaliação de riscos: análise qualitativa e quantitativa, considerando probabilidade e impacto.

➢ Resposta a riscos: definição de estratégias (evitar, reduzir, compartilhar ou aceitar), incluindo procedimentos para resposta a incidentes de dados pessoais, em conformidade com a LGPD e comunicação à ANPD e aos titulares, quando aplicável.

➢ Priorização de riscos: com destaque para riscos que envolvam dados pessoais sensíveis.

➢ Controles internos: implementação de políticas de privacidade, segurança da informação, controle de acesso e registro de operações de tratamento de dados.

➢ Informação e comunicação: garantir que informações relevantes circulem de forma clara e tempestiva, incluindo dados relativos a incidentes de privacidade.

➢ Monitoramento: revisão contínua dos controles internos e do plano de resposta a incidentes de dados.

5. CONTROLES INTERNOS

Os Controles Internos foram estruturados para oferecer segurança razoável ao alcance dos objetivos da empresa.

Contemplam, além dos aspectos tradicionais de gestão de riscos:

- Políticas de privacidade e segurança da informação;

- Procedimentos de resposta a incidentes de dados;

- Registros de operações de tratamento de dados pessoais;

- Garantia de direitos dos titulares de dados (acesso, correção, exclusão, portabilidade).

6. DAS RESPONSABILIDADES

- Os gestores de cada setor da BRS SUPRIMENTOS CORPORATIVOS são responsáveis pelo gerenciamento dos riscos, incluindo riscos relacionados ao tratamento de dados pessoais.

- Compete a todos os colaboradores monitorar riscos corporativos e de privacidade, reportando fragilidades e incidentes.

- A BRS SUPRIMENTOS CORPORATIVOS mantem um Encarregado de Proteção de Dados (DPO), conforme previsto na LGPD, responsável por:

- Receber comunicações de titulares e da ANPD;

- Orientar colaboradores sobre práticas de proteção de dados;

- Apoiar na gestão de incidentes e conformidade regulatória.

Este documento entra em vigor a partir da sua aprovação pela alta administração e substitui versões anteriores.

Política de Privacidade	Versão: 2.0	Data: 04/11/2024
Autor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Revisor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Classificação da informação: Pública		

POLÍTICA DE PRIVACIDADE

BRS SUPRIMENTOS CORPORATIVOS S/A

1. INTRODUÇÃO

A BRS SUPRIMENTOS CORPORATIVOS valoriza a privacidade e a proteção de dados pessoais, comprometendo-se a adotar as melhores práticas e cumprir integralmente a Lei Geral de Proteção de Dados (LGPD - Lei nº 13.709/2018). Esta política explica como coletamos, utilizamos, armazenamos e compartilhamos informações pessoais.

Ao utilizar nossos serviços, o USUÁRIO declara estar ciente e de acordo com os termos desta Política de Privacidade.

2. COLETA E USO DE DADOS PESSOAIS

2.1. Dados Coletados

Os dados pessoais podem ser coletados por meio do nosso site, e-mails ou interações diretas, incluindo:

- Dados de identificação: Nome, CPF, RG, endereço, telefone, e-mail.
- Dados sensíveis: Informações de saúde, registros financeiros e outros, conforme necessidade específica e autorização prévia do titular.
- Dados profissionais: Experiência, formação e informações de candidatos.

2.2. Finalidade do Uso dos Dados

Utilizamos os dados para:

- Cumprir obrigações contratuais e legais.
- Garantir segurança e identificar os usuários.
- Melhorar nossos serviços e atendimento.
- Realizar comunicações institucionais, comerciais ou de marketing, com consentimento prévio.

3. ARMAZENAMENTO E SEGURANÇA

3.1. Local de Armazenamento

Os dados são armazenados em ambientes seguros, podendo incluir servidores no Brasil ou em provedores de nuvem localizados em outros países que garantam níveis adequados de proteção.

3.2. Prazo de Retenção

- Dados pessoais serão mantidos pelo período necessário para atender às finalidades descritas nesta política, respeitando prazos legais aplicáveis.
- Após o prazo, os dados serão anonimizados ou excluídos de forma segura.

3.3. Medidas de Segurança

Adotamos medidas técnicas e administrativas para proteger os dados contra acessos não autorizados, perdas ou vazamentos, incluindo:

- Controle de acessos.
- Criptografia.
- Monitoramento contínuo.

4. DIREITOS DO TITULAR DOS DADOS

Os titulares dos dados possuem os seguintes direitos, conforme a LGPD:

- Confirmar a existência de tratamento de seus dados.
- Acessar, corrigir ou solicitar a exclusão de seus dados.
- Solicitar a portabilidade dos dados.
- Opor-se ao tratamento de dados em determinadas circunstâncias.
- Retirar consentimento a qualquer momento.

Para exercer seus direitos, o titular pode entrar em contato com nosso Encarregado de Proteção de Dados pelo canal: [inserir canal de contato].

5. COMPARTILHAMENTO DE DADOS

5.1. Com quem Compartilhamos

Os dados podem ser compartilhados com:

- Autoridades competentes, mediante exigência legal.
- Terceiros contratados para serviços relacionados às finalidades mencionadas (ex.: provedores de TI, consultorias).
- Empresas do mesmo grupo econômico.

5.2. Transferências Internacionais

A empresa não transfere dados internacionalmente.

6. ALTERAÇÕES DA POLÍTICA

Reservamo-nos o direito de alterar esta Política de Privacidade a qualquer momento, garantindo transparência e comunicação prévia ao titular quando mudanças significativas forem realizadas.

7. DISPOSIÇÕES FINAIS

Esta Política será regida pela legislação brasileira. Em caso de dúvidas, reclamações ou solicitações, entre em contato com nosso Encarregado de Proteção de Dados.

Política de Segurança da Informação	Versão: 2.0	Data: 07/10/2024
Autor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Revisor: BRS SUPRIMENTOS CORPORATIVOS S/A		
Classificação da informação: Pública		

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

BRS SUPRIMENTOS CORPORATIVOS S/A

1. Introdução

A política de segurança da informação da BRS SUPRIMENTOS CORPORATIVOS adota critérios técnicos e administrativos aptos a proteger os dados pessoais contra acessos não autorizados e incidentes de destruição, perda, alteração ou divulgação indevida, de acordo com o Art. 46 da LGPD. A empresa visa garantir a segurança dos dados por meio de controles técnicos e organizacionais, em conformidade com normas como a ISO 27001.

2. Objetivo

Esta política tem como objetivo definir diretrizes de proteção de dados pessoais, sensíveis ou não, utilizados nos processos da BRS SUPRIMENTOS CORPORATIVOS. A empresa se compromete a adotar medidas apropriadas para assegurar a confidencialidade, integridade, disponibilidade e transparência no tratamento de dados pessoais, garantindo o direito dos titulares.

3. Abrangência

Aplica-se a todos os usuários internos e externos que, de alguma forma, tenham acesso aos sistemas e dados controlados pela BRS SUPRIMENTOS CORPORATIVOS. Todos os colaboradores, prestadores de serviço e parceiros que tratam dados devem estar cientes das suas responsabilidades sob a LGPD.

4. Diretrizes Gerais

4.1. Princípios de tratamento de dados

O tratamento de dados pessoais na BRS SUPRIMENTOS CORPORATIVOS respeitará os princípios da LGPD, incluindo **finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação e responsabilização**. A coleta e tratamento de dados pessoais somente ocorrerão mediante **consentimento explícito**, ou quando houver base legal adequada.

4.2. Proteção de dados pessoais

Os dados pessoais serão tratados de forma segura, utilizando sistemas de autenticação, criptografia e medidas de controle de acesso restrito. A empresa aplicará boas práticas para garantir que somente dados essenciais sejam coletados, e que eles sejam utilizados exclusivamente para finalidades previamente estabelecidas, informadas e autorizadas pelo titular.

4.3. Gestão de consentimento

A obtenção de consentimento será realizada de forma clara e objetiva, e o titular dos dados terá o direito de revogar seu consentimento a qualquer momento, conforme o Art. 8 da LGPD. Para dados pessoais sensíveis, será exigido consentimento específico e destacado, conforme estipulado pelo Art. 11.

4.4. Direitos dos titulares dos dados

A BRS SUPRIMENTOS CORPORATIVOS assegura aos titulares de dados o exercício dos seus direitos conforme o Capítulo III da LGPD. Isso inclui o direito de acessar, corrigir, eliminar, e solicitar a portabilidade dos dados, bem como obter

informações claras sobre o tratamento dos seus dados pessoais. Os titulares também poderão solicitar a revisão de decisões automatizadas.

4.5. Tratamento de dados sensíveis e transferência internacional

O tratamento de dados pessoais sensíveis será realizado com cuidado redobrado, e a transferência internacional de dados pessoais só ocorrerá para países que garantam níveis de proteção de dados adequados, conforme os requisitos do Capítulo V da LGPD.

4.6. Incidentes de segurança e notificação

Em caso de incidente de segurança que possa acarretar risco ou dano aos titulares dos dados, a BRS SUPRIMENTOS CORPORATIVOS compromete-se a notificar a Autoridade Nacional de Proteção de Dados (ANPD) e os titulares dos dados afetados, conforme determina o Art. 48 da LGPD. Para tal, será mantido um plano de resposta a incidentes, incluindo medidas corretivas e preventivas.

5. Governança e Responsabilidade

5.1. Encarregado de proteção de dados (DPO)

A BRS SUPRIMENTOS CORPORATIVOS nomeou um Encarregado de Proteção de Dados (DPO), que é o responsável por assegurar a conformidade com a LGPD, bem como por atender solicitações de titulares e autoridades competentes.

5.2. Treinamento e conscientização

Serão realizados treinamentos periódicos com todos os colaboradores sobre a importância da proteção de dados pessoais e a observância dos direitos dos titulares de dados sob a LGPD.

6. Armazenamento e Eliminação de Dado

Os dados pessoais serão armazenados apenas pelo tempo necessário para cumprir as finalidades informadas e autorizadas pelo titular, observando-se os prazos legais e regulamentares. Após o cumprimento dessas finalidades, os dados deverão ser eliminados ou anonimizados, conforme previsto no **Art. 16 da LGPD.

Essa versão da política reforça a proteção de dados pessoais em conformidade com a LGPD, garantindo que todos os processos que envolvem dados pessoais sejam conduzidos de maneira segura, ética e transparente.