POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PSI

1.	OBJETIVO	3
2.	RESPONSABILIDADES	3
3.	ACESSO E AUTENTICAÇÃO	4
4.	SENHAS	4
5.	E-MAIL CORPORATIVO	5
6.	ACESSO A INTERNET	5
7.	USO DE ESTAÇÃO DE TRABALHO E DISPOSITIVOS MÓVEIS	6
8.	ACESSO FÍSICO	7
9.	FIREWALL	7
10.	ACESSO REMOTO E TELETRABALHO	9
11.	USUÁRIOS PRIVILEGIADOS E CONTAS GENÉRICAS	9
12.	ENGENHARIA SOCIAL	10
13.	VÍRUS E CÓDIGOS MALICIOSOS	10
14.	ENTRADA E SAÍDA DE COLABORADORES (CONCESSÃO E REVOGAÇÃO DE ACESSOS)	11
15.	REVISÃO DE ACESSOS	12
16.	GESTÃO DE VULNERABILIDADES	12
17.	TERMOS E DEFINIÇÕES	13
	SUPORTE E COMUNICAÇÃO	18
	MEMBROS DA EQUIPE DE TI	18
	MEMBROS DA EQUIPE DE SEGURANÇA DA INFORMAÇÃO E PROTEÇÃO DE DADOS PESSOAIS	18

1. OBJETIVO

A segurança é um dos assuntos mais importantes dentre as preocupações de qualquer empresa. O Objetivo dessa Política de Segurança da Informação, PSI, é apresentaremos um conjunto de regras, instruções e procedimentos para aderir os requerimentos de negócio baseado nos pilares da Segurança da informação CID (Confidencialidade, Integridade, Disponibilidade), protegendo os ativos da empresa, sejam digitais, virtuais, físicos ou analógicos.

A empresa e a política de segurança

Essa política (PSI), e todas as normas aqui estabelecidas, se aplicam a todos ativos, e colaboradores da BESTCRED, sejam contratados diretos, como funcionários, parceiros ou prestadores de serviços.

Onde todos devem respeitar todos os tópicos aqui abordados, e cientes de que seus os ativos e sistemas, como: e-mails e navegação na internet/intranet são monitorados. A equipe de segurança da informação (SI) ou tecnologia (TI), encontram-se a total disposição para saneamento de dúvidas e auxílio técnico.

2. RESPONSABILIDADES

A Diretoria da BESTCRED em conjunto com o responsável pela área de Tecnologia, são responsáveis por manter essa política atualizada e alinhada com os objetivos de negócio em conformidade com a Segurança da informação.

Todos os usuários de sistemas da BESTCRED são responsáveis por zelar essa PSI. O não cumprimento dessas políticas poderá acarretar sanções administrativas em primeira instância, podendo ocasionar o desligamento do colaborador/prestador de acordo com a gravidade da ocorrência

3. ACESSO E AUTENTICAÇÃO

O Acesso a todos sistemas e ativos da BESTCRED, deve possuir uma credencial exclusiva, que identifique para fins de proteção, identificação e registro de atividades realizadas.

Todo colaborador e usuário de sistemas da BESTCRED, possuirá uma credencial em formato de *login* pessoal, intransferível, com uma senha única. É proibido compartilhá-la, divulgá-la ou anotá-la visivelmente em qualquer ambiente ou meio.

A autenticação no sistema de informática é baseada em uma senha, seguida de seu *login*. Esse meio é muito utilizado por sua facilidade de implantação e manutenção. Não é permitido o uso de sistemas, sem identificação ou autenticação antes da entrada / *login,* nos sistemas.

4. SENHAS

Não é permitido senhas simples como nome do usuário, combinações simples (abc123), substantivos (casa, meia, cadeira, brasil), datas (11092001). É necessário criar senha forte, observando as regras da política de senhas:

- Uma senha segura deverá conter no **mínimo 8** caracteres alfanuméricos (letras e números) com diferentes caixas. Utilize padrões como dos exemplos:
    - eSuo8Car (eu SEMPRE uso oito 8 Caracteres)
    - odIamp0709 (ouviram do Ipiranga as margens plácidas 7 de setembro) @s3Nh45@ (A palavra senhas onde o 3 substitui o E, o 4 o A, e o 5 o S
- As senhas terão um tempo de vida útil determinado pela equipe de segurança. A acesso principale central (Rede), renovar a senha automaticamente a cada 42 dias, devendo o mesmo ser respeitado, caso contrário o usuário ficará sem acesso aos sistemas.

Sua senha não deve ser jamais passada a ninguém, nem mesmo da equipe de segurança. Caso desconfie que sua senha não está mais segura, sinta-se à vontade para alterá-la, mesmo antes do prazo determinado de validade.

Tudo que for executado com a sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para manter sua senha secreta.

5. E-MAIL CORPORATIVO

O uso do email corporativo oficial @bestcred.com.br, deve ser restrito a suas atividades de trabalho, sendo proibido para fins pessoais. As seguintes regras e boas práticas para uso de e-mail devem ser respeitadas:

- Não abra anexos com as extensões .bat, .exe, .src, .lnk e .com
- Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês.
- Alguns dos vírus mais terríveis dos últimos anos tinham assuntos como: ILOVEYOU, Branca de neve pornô, etc.
- Não reenvie e-mails do tipo corrente, aviso de vírus, avisos da Microsoft/AOL/Symantec, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, etc.
- Não mande e-mails para mais de 10 pessoas de uma única vez (to, cc, bcc)
- Evite anexos muito grandes, acima de 25 MBytes.

É proibido o uso de e-mails pessoais, para exercer as atividades de trabalho da BEST, transmitir arquivos ou informações da empresa e seus clientes.

6. ACESSO A INTERNET

A Internet deve ser utilizada para realizar suas atividades no trabalho. As seguintes regras e boas práticas para uso da internet devem ser respeitadas:

- O uso recreativo da internet não deverá se dar no horário de expediente.
- Somente navegação de sites é permitida (www. Http, https). Casos específicos que exijam outros protocolos deverão ser solicitados diretamente a equipe de segurança com prévia autorização do

supervisordo departamento local.

- Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará bloqueado e monitorado
- É proibido o uso de ferramentas P2P (kazaa, Morpheus, etc)
- É proibido o uso de IM (Instant messengers) não homologados/autorizados pela equipe de segurança

O uso da internet é registrado em históricos e logs, e pode ser auditado pela empresa a qualquer momento.

7. ESTAÇÃO DE TRABALHO CORPORATIVA, DISPOSITIVOS MÓVEIS E PESSOAIS

Cada estação de trabalho tem códigos internos que permitem que o equipamento seja identificada na rede da BEST. Cada indivíduo possui sua própria estação de trabalho (desktop) ou móvel (laptop), para realizar suas atividades. Cada colaborador é responsável pelo zelo do equipamento, utilização adequada e informações contidas.

Os equipamentos pessoais, computadores, laptops ou celulares, por padrão, não são utilizados e permitidos para acessar os sistemas da BEST. Qualquer excessão deverá ser solicitada formalmente e autorizada pelas áreas de RH e TI, para medidas adicionais de segurança e controle.

As seguintes regras e boas práticas para uso dos computadores devem ser respeitadas:

- Ao sair da frente de sua estação, tenha certeza de que tenha feito o “log off”, ou bloqueou a tela de espera com senha;
- Não instale nenhum tipo de software / hardware sem autorização da equipe técnica ou de segurança

- Não tenha MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de pirataria
- Todos arquivos de trabalho devem ser salvos nas pastas da rede ou sharepoint, onde está protegida

por controle de acesso e backup

- Todos computadores da empresa devem possuir um sistema de proteção antimalware
- Por padrão, as unidades de armazenamentos removíveis e Discos são bloqueados (Pen-Drives, HD´s Usb, DVD-R), qualquer necessidade específica deve ser solicitada formalmente ao RH e TI, para posterior análise e autorização

Os equipamentos pessoais, computadores, laptops ou celulares, por padrão, não são utilizados e permitidos para acessar os sistemas da BEST. Qualquer excessão deverá ser solicitada formalmente e autorizada pelas áreas de RH e TI, para medidas adicionais de segurança e controle.

8. ACESSO FÍSICO

Todos sistemas vitais da empresa, como servidores, links, firewalls, devem possuir sala protegida e adequada seguindos as seguintes regras:

- Sala exclusiva, restrita e fechada com chaves para guarda dos equipamentos
- Chaves com acesso restrito ao pessoal do Depto de TI
- Sistema de Proteção de Energia (Nobreak)
- Ar-Condicionado exclusivo
- RACK, ou Armário adequado para equipamentos eletrônicos
- Identificação e Etiquetação de todos ativos/equipamentos
- Documentação dos equipamentos (topologia)
- Qualquer manuteção, instalação ou prestador terceiro, deve estar acompanhado do TI

9. FIREWALL

Todo o ambiente de sistemas da BESTCRED, que possuir links de acesso a Internet, redes externas, e servidores deve possuir um firewall instalado para proteção de perímetro e controle. O Firewall determina à política de uso de acesso à Internet e Sistemas de todos os colaboradores. Os acessos são classificados e divididos baseado em nas funções e atividades necessárias para os colaboradores execerem suas atividades especificas da empresa.

A regra utilizada é a *RBAC* (Role Base Access Control). Onde há níveis de acesso no sistema, com permissões ou bloqueios conforme área ou equipe de trabalho. Demonstrado na tabela abaixo:

GRUPO	Origem	Navegação	Email	Redes Sociais	Acesso Restrito aSites	Filtros
A	Servidores, Rede	SIM	SIM	NÃO	NÃO	SIM
B	Diretores	SIM	SIM	SIM	NÃO	NÃO
C	Supervisores	SIM	SIM	SIM	NÃO	SIM
D	Analistas	SIM	SIM	NÃO	SIM	NÃO
E	Estagiários	NÃO	NÃO	NÃO	SIM	SIM

- Acesso Restrito a Sites: conceito de acesso somente com cadastros prévios de sites liberados para uso (whitelist).
- Filtro: conceito de bloquear somente sites ou categorias marcadas (Blacklist), exemplo: Jogos, pornô.

O Firewall possui uma central de histórico de uso (Logs), para efeitos de controle e auditoria de utilização

da internet pelos colaboradores e sistemas. Todos as configurações de acesso internet, serviços e rotas de conexão a Internet ou Intranet, através do Firewall, são revisadas no mínimo anualmente, e gerenciadas pelo Responsável da Tecnologia.

10. ACESSO REMOTO E TELETRABALHO

O Acesso remoto ou Teletrabalho à rede da Bestcred, deve ser feito através de conexãos segura, como VPN (RedeVirtual Remota), onde possua:

- Autorização do Gestor da área, explicando a necessidade
- Credencial exclusiva para a VPN por usuário nominado
- Senha exclusiva da VPN, com login diferente da rede
- Registro de acessos através de log ou Monitoramento especial

11. ACESSOS PRIVILEGIADOS E CONTAS GENÉRICAS

Todos os acessos de contas privilegiadas dos sistemas da BESTCRED, equivalentes a *super usuário*, administradores (*admin*), devem respeitar as seguintes regras:

- Ser restrito ao responsável pela área de Tecnologia, ou dono do sistema
- Uso exclusivo para fins de configuração e ajustes do sistema, mas não para seu uso diário (*um usuário complementar e individual de TI deve ser aplicado para uso diário)*
- Possuir senha complexa, e diferente para cada sistema
- Mais do que um fator de Autenticação do *login* de nome+senha (Código via SMS, E-Mail, token, certificado digital)

Todas as contas genéricas, ou de sistemas, devem ser exclusivas e usadas em situações especificas, e estritamente necessárias, e devem ser controladas pelo departamento de Tecnologia. Exemplos aceitáveis de contas genéricas: digitalização (Scanner), impressão em rede.

12. ENGENHARIA SOCIAL

Como seres humanos, temos a grande vantagem de sermos sociáveis, mas muitas vezes quando o assunto é sobre segurança, isso é uma desvantagem. Por isso observe os seguintes cuidados com a engenharia social:

- Não fale sobre a política de segurança da empresa com terceiros ou em locais públicos.
- Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha.
- Não digite suas senhas ou usuários em máquinas de terceiros, especialmente fora da empresa.
- Somente aceite ajuda técnica de um membro de nossa equipe técnica previamente apresentado e identificado.
- Nunca execute procedimentos técnicos cujas instruções tenham sido recebidas por e-mail.
- Relate a equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

13. VÍRUS E CÓDIGOS MALICIOSOS

Todos os ativos e sistemas da BESTCRED, devem ter um sistema de *antimalware*, para proteção das informações. As sseguintes regras devem ser utilizadas e seguidas pelo sistema de antimalware da empresa:

- Proteção em Tempo Real
- Atualização automática, mínimo uma vez ao dia
- Proteção e bloqueio de execução de dispositivos móveis, USB e armazenamentos remotos
- Não clicar em links dentro de e-mails
- Reportar atitudes suspeitas em seu sistema a equipe de tecnologia, para que possíveis vírus possam ser identificados no menor espaço de tempo possível

- Não utilize pendrives ou DVDs/CDs de fora da empresa

Caso isso seja extremamente necessário, encaminhe o mesmo para a equipe técnica, onde passará por uma verificação antes de ser liberado para uso.

14.ENTRADA E SAÍDA DE COLABORADORES (CONCESSÃO E REVOGAÇÃO DE ACESSOS)

Toda movimentação de colaboradores - entrada ou saída – na BESTCRED, deve ter um chamado registrado pelo Gestor de Recursos Humanos (RH), ou Gestor Operacional, via helpdesk ou e- mail para o TI, com uma antecedência mínima de 3 dias.

O processo de entrada, significa concessão de acesso. Onde o Gestor do RH deverá especificar os dados abaixo registrando no chamado:

- Nome Completo
- Equipe / Departamento / Área
- Função

Compete ao Gestor da Equipe solicitar via helpdesk, os recursos adicionais ou específicos para o colaborador (Acesso a pastas na rede, acesso VPN, ramal).

A criação de login de usuários nos sistemas obedecerá a seguinte regra:

- Primeiro Nome + Último Sobrenome, ex.: João da Silva, usuário = *joaosilva*.

O Departamento de Tecnologia gera um TERMO DE RESPONSABILIDADE, com a descrição dos ativos e sistemas de uso para o novo colaborador assinar.

O processo de saída, significa revogação de acesso. Onde o Gestor do RH deverá especificar o os dados abaixo no chamado:

- Nome Completo
- Equipe / Departamento / Área
- Função

15. REVISÃO DE ACESSOS PERIÓDICO

Mensalmente o Departamento de Recursos Humanos ou Gestor operacional, encaminha uma listagem de colaboradores ativos atualizada para o departamento de tecnologia. Em posse dessa lista o departamento de TI realiza a revisão dos logins ativos nos sistemas, a fim de desativar/cancelar acessos de ex-colaboradores, para reduzir qualquer risco de acesso indevido aos sistemas da Empresa.

16. GESTÃO DE VULNERABILIDADES

A gestão de vulnerabilidades dos sistemas da BESTCRED, dever ser feitas no mínimo 1 x ao ano, por profissional autônomo especialista em Segurança da Informação, ou por um sistema automatizado.

O processo de identificação de vulnerabilidades deve:

a. Mapear e identificar ativos que possam conter vulnerabilidades à Segurança da Informação, incluindo ambientes físicos ou lógicos, como:
   i. Servidores
   ii. Firewalls
   iii. Sistemas Administrativos - Financeiros (ERP/CRM)
   iv. Links de Acesso à Internet
   v. Cópias de Segurança
   vi. Wifi
   vii. CPD

b. Considerar as vulnerabilidades publicadas no mercado.

O Resultado da análise deve ser reportado para a Diretoria e a área de Tecnologia, para que planejem as melhorias ou correções necessárias, levando em conta a Criticidade conforme tabela:

	Criticidade
Alto	A correção deve ser aplicada em até 30 dias.
Médio	A correção deve ser aplicada em até 60 dias.
Baixo	A correção deve ser aplicada em até 90 dias.

17. TERMOS E DEFINIÇÕES

Acordo de Sigilo e Responsabilidade: Acordo assinado pelo colaborador e prestador de serviço para firmar seu compromisso com o sigilo das informaçõesda empresa e dos clientes.

Ameaças Virtuais: Programas maliciosos que têm como objetivo burlar a Segurança da Informação e atacar os ativos, impactando sua confidencialidade, integridade ou disponibilidade.

Ativos de Informação: qualquer recurso que tenha a condição de processar,armazenar ou transmitir informação e a sua própria informação.

Antivírus: Programa instalado no computador para proteger as informações emanter nossa máquina segura.

Ambiente Lógico: Ambiente virtual composto pelos Recursos de TIC, sistemas,bases de dados, do **BESTCRED**, de forma intangível.

Ameaça: Causa potencial de um incidente indesejado, que pode resultar emdano ao **BESTCRED**.

Aplicativos de Comunicação Instantânea: Conjuntos de códigos e instruções compilados, executados ou interpretados por um Recurso de Tecnologia da Informação e Comunicação, armazenados em um dispositivo ou na nuvem, que são usados para troca rápida de mensagens, conteúdos e informações multimídia.

Ativo: É qualquer coisa que tenha valor para o **BESTCRED** e precisa ser adequadamente protegido.

Ativo Intangível: Todo elemento que possui valor para o **BESTCRED** e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando a dados, reputação, imagem, marca e conhecimento.

Autenticidade: Garantia de que a informação foi criada, editada ou emitida por quem se disse ter sido, sendo capaz de gerar evidências não repudiáveis em relação ao criador, editor ou emissor.

***Backup*:** Salvaguarda de informações realizada por meio de reprodução e/ou espelhamento de uma base de arquivos com a finalidade de plena capacidade de recuperação em caso de incidente ou necessidade de *restore*, ou ainda,

constituição de infraestrutura de acionamento imediato em caso de incidente ou necessidade justificada do **BESTCRED**.

Classificação da Informação: atividade de inventariar e categorizar as informações, definir seu grau de sensibilidade e o grupo de acesso.

Colaborador: Empregado, estagiário, prestador de serviço, terceirizado, fornecedor, menor aprendiz ou qualquer outro indivíduo ou organização que venha a ter relacionamento profissional com o **BESTCRED,** direta ou indiretamente.

Confidencialidade: Garantia de que as informações sejam acessadas somente por aqueles expressamente autorizados e que sejam devidamente protegidas do conhecimento dos não

autorizados.

Credencial de Acesso: É a identificação do colaborador em ambientes lógicos, sendo composta por seu nome de usuário (login) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificadodigital, token e biometria.

Criptografia: Técnica utilizada para garantir a segurança das informações e permitir que somente pessoas autorizadas consigam acessá-las.

Disponibilidade: Garantia de que as informações e os recursos de TIC estejam disponíveis sempre que necessário e mediante a devida autorização para seu acesso ou uso.

Dispositivos Móveis: equipamentos que podem ser facilmente transportados devido a sua portabilidade, com capacidade de registro, armazenamento ou processamento de informações, além da possibilidade de estabelecer conexõescom a Internet e outros sistemas, redes ou qualquer dispositivo.

Dispositivos Removíveis de Armazenamento de Informação: Dispositivos capazes de armazenar informações que pode ser removida do equipamento, possibilitando a portabilidade dos dados, como CD, DVD e *pen drive*.

Download: Transferência de informações de um programa ou arquivo para o computador.

Evento de Segurança da Informação: Ocorrência identificada de um sistema, serviço ou rede, que indica uma possível violação da política da segurança da informação ou falha nos controles, ou uma situação previamente desconhecida, que possa ser relevante para a Segurança da Informação. Incidente ocorrido no ambiente que gerou consequências para a confidencialidade, integridade ou disponibilidade de um ativo.

Homologação: Processo de avaliação e aprovação técnica de **recursos de TIC** para serem utilizados dentro do ambiente do **BESTCRED**.

Identidade Digital: É a identificação do Colaborador em ambientes lógicos, sendo composta por seu nome de usuário (*login*) e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificadodigital, *token* e biometria.

Incidente de Segurança da Informação: Ocorrência identificada de um estado de sistema, dados, informações, serviço ou rede que indica possível violação à Política de Segurança da Informação ou documentos complementares, falha de controles ou situação previamente desconhecida e que possa ser relevante à segurança da informação.

Informação: É o conjunto de dados que, processados ou não, podem ser utilizados para produção, transmissão e compartilhamento de conhecimento, contidos em qualquer meio, suporte ou formato.

Integridade: Garantia de que as informações estejam fidedignas em relação à última alteração desejada durante o seu ciclo de vida.

Internet: Rede mundial de computadores interconectada pelo protocolo TCP/IP cuja infraestrutura tem caráter aberto e colaborativo, acessível por meio de dispositivos com conexão e autorizações suficientes e que permite obter informação de qualquer outro dispositivo que também esteja conectado à rede,desde que configurado adequadamente.

Legalidade: Garantia de que todas as informações sejam criadas e gerenciadas de acordo com as disposições do ordenamento Jurídico em vigor.

Mídias Sociais: plataformas ou aplicativos baseados em Internet, sobre os quais ocorrem a interação entre pessoas físicas ou jurídicas com a produção, troca e compartilhamento de informações de modo descentralizado. Exemplo: Instagram, Facebook, LinkedIn, Yammer, Twitter e Snapchat.

Política: Conjunto de diretrizes sobre um determinado assunto. Ela fornece parâmetros e orientações para a tomada de decisões e é à base de sustentação para o planejamento estratégico.

Recursos de Tecnologia da Informação e Comunicação (Recursos de TIC): São todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação. Entre os tipos de recursos podemos destacar: computares de mesa ou portáteis, *smartphones, tablets, pen drive,* discos externos, mídias, impressoras, *scanner*,

entre outros. Sempre que mencionados de forma a não identificar seu possuidor ou proprietário, os **Recursos de TIC** compreenderão tanto os pertencentes ao **BESTCRED** quanto aos particulares em proveito corporativo. Caso contrário, haverá declinação de posse ou propriedade no próprio texto.

Repositórios Digitais (*Cyberlockers*): Plataformas de armazenamento na Internet, a exemplo, mas não se limitando ao *Google Drive, OneDrive, Dropbox, iCloud, Box*, *SugarSync*, *Slideshare* e *Scribd.*

Risco: Combinação da probabilidade da concretização de uma ameaça e seus potenciais impactos.

Tentativa de Burla: Atos que busquem violar as diretrizes estabelecidas nos documentos normativos do **BESTCRED** e sejam frustrados por erro durante o planejamento ou durante sua execução.

Tratamento da Informação: uso adequado da informação de acordo com as diretrizes estabelecidas nos diversos cenários que ocorrem no dia a dia (armazenamento, transmissão, descarte, impressão etc...)

Violação: Qualquer atividade que desrespeite as regras estabelecidas nos documentos normativos do **BESTCRED**.

Vírus: Programas maliciosos desenvolvidos para danificar o computador e alterar seu funcionamento.

Suporte e Comunicação

As informações relacionadas a PSI devem estar disponíveis e em fácil acesso para 100% da equipe de colaboradores, assim como todo e qualquer tipo de suporte precisa ocorrer para que não haja o descumprimento das regras por falta ou desatualização de informações. Por isso nossa equipe de TI e de segurança contam com a sua colaboração para manter nossa empresa segura.

Entre em contato conosco via helpdesk, sempre que julgar necessário e/ou precisar de ajuda.

Membros da equipe de TI

Responsável pela área de Tecnologia: Thiago CoelhoE-mail tiago.coelho@bestcredsp.com.br

Ramal 3101-4912

Membros da equipe de Segurança da Informação e Proteção de Dados Pessoais

Nome Vanessa Nascimento

E-mail dpo@bestcredsp.com.br

NATUREZA DA REVISÃO

Revisão	Data	Descrição da Revisão
1	**01.04.21**	Criação do Documento
2 e 3	**03.04.22**	Atualização e adequação de Formato
4	**29.05.23**	Atualização da Política
5	**17.05.24**	Atualização da Política