

# POLÍTICA EMPRESARIAL



## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023

# POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Copyright©: NOVO CONCEITO

# POLÍTICA EMPRESARIAL



*Novo Conceito*

## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023

<b>1</b>	<b>OBJETIVO</b>	<b>3</b>
<b>2</b>	<b>ABRANGÊNCIA</b>	<b>4</b>
<b>3</b>	<b>DEFINIÇÕES</b>	<b>4</b>
<b>4</b>	<b>DIRETRIZES</b>	<b>5</b>
<b>4.1</b>	<b>PILARES DA SEGURANÇA DA INFORMAÇÃO</b>	<b>5</b>
<b>4.2</b>	<b>ASPECTOS GERAIS</b>	<b>6</b>
<b>4.3</b>	<b>GESTÃO DE ACESSOS E IDENTIDADE</b>	<b>7</b>
<b>4.4</b>	<b>GESTÃO DE CORREIO ELETRÔNICO (E-MAIL)</b>	<b>8</b>
<b>4.5</b>	<b>TRATAMENTO DA INFORMAÇÃO</b>	<b>9</b>
<b>4.6</b>	<b>GESTÃO DE RISCOS, OBJETIVOS E INCIDENTES DE SEGURANÇA DA INFORMAÇÃO</b>	<b>9</b>
<b>4.7</b>	<b>TREINAMENTOS DE CONSCIENTIZAÇÃO</b>	<b>9</b>
<b>4.8</b>	<b>RESPONSABILIDADES</b>	<b>10</b>
<b>5</b>	<b>AÇÕES DE GERENCIAMENTO</b>	<b>11</b>
<b>6</b>	<b>DISPOSIÇÕES GERAIS</b>	<b>11</b>
<b>7</b>	<b>APROVAÇÕES</b>	<b>12</b>

# POLÍTICA EMPRESARIAL



## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023

### 1 OBJETIVO

---

Esta política estabelece os conceitos e diretrizes de segurança da informação, visando proteger as informações da **NOVO CONCEITO** e de seus clientes. Posiciona-se como documento estratégico, com vistas a promover o uso seguro dos ativos de informação da **NOVO CONCEITO**. Assim, deve ser entendida como uma declaração formal da Alta Administração acerca de seu compromisso com a proteção das informações sobre sua custódia, devendo ser cumprida por todos os colaboradores, e colaboradores terceirizados da **NOVO CONCEITO**.

A política foi baseada em:

- Soluções (SaaS), onde todos os recursos estão na Nuvem e são oferecidos por um player de mercado (denominado: fornecedor). No modelo SaaS (Software as a Service), as responsabilidades de manter o ambiente seguro e atualizado são totalmente do provedor. A **NOVO CONCEITO** deve garantir que esteja de acordo com as normas de segurança adotada pelo fornecedor e aplicar as recomendações quando necessárias e pertinentes ao negócio.
- A Equipe da **NOVO CONCEITO** é composta por colaboradores contratados nas modalidades PJ (Pessoa Jurídica) e CLT com equipamentos fornecidos pela empresa, contam com suporte técnico oferecido pela **NOVO CONCEITO** que é responsável pelas atualizações definidas relacionadas à segurança, configurações de acessos, e-mail, antivírus etc.
- O antivírus por ser uma ferramenta essencial para a segurança da informação, será oferecido pela **NOVO CONCEITO**, mesmo que a modalidade de trabalho seja BYOD.

**Esta política foi aprovada pelo Comitê de Segurança da Informação da NOVO CONCEITO.**

# POLÍTICA EMPRESARIAL



## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023

## 2 ABRANGÊNCIA

---

A Política de Segurança da Informação na **NOVO CONCEITO** aplica-se a todos os colaboradores, prestadores de serviços, sistemas e serviços incluindo trabalhos executados externamente ou por terceiros que utilizem o ambiente de processamento da **NOVO CONCEITO** ou acesso às informações pertencentes a empresa e seus clientes. A observância destas diretrizes é obrigatória e reflete a Governança Corporativa acerca dos temas de Segurança da Informação Corporativa da **NOVO CONCEITO**.

Após a leitura desta política, os integrantes/usuários, colaboradores e executivos devem assinar a Política de Segurança da Informação para confirmar que a mensagem da política foi compreendida e se refletirá em suas atitudes.

### **A violação desta política de segurança é qualquer ato que:**

- 2.1 *Exponha a Companhia a uma perda monetária efetiva ou potencial por meio do comprometimento da segurança dos dados/informações ou ainda da perda de equipamento.*
- 2.2 *Envolva a revelação de dados confidenciais, direitos autorais, negociações, patentes ou uso não autorizado de dados corporativos.*
- 2.3 *Envolva o uso de dados para propósitos ilícitos, que venham a incluir a violação de qualquer lei, regulamento ou qualquer outro dispositivo governamental.*

## 3 DEFINIÇÕES

---

**Segurança da Informação** – Visa a preservar as propriedades de confidencialidade, integridade, disponibilidade, não se limitando a sistemas computacionais, informações eletrônicas e/ou sistemas de armazenamento.

# POLÍTICA EMPRESARIAL



## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023

## 4 DIRETRIZES

---

A **NOVO CONCEITO** é comprometida com a observância da legislação em vigor aplicável, bem como do Estatuto da Companhia e do Código de Ética e Conduta da ABEP (Associação Brasileira de Empresas de Pesquisa). E para a condução de suas atividades empresariais é necessário o estabelecimento de uma Política de Segurança da Informação estruturada e clara que possibilite aderência e conformidade, tendo como referência:

- Norma ISO/IEC 27001, cláusulas 2 e 5.3
- Norma ISO/IEC 27017
- Lista de obrigações Legais, Regulamentares e Contratuais

### 4.1 Pilares da Segurança da Informação

A segurança da informação é aqui caracterizada pela preservação dos seguintes pilares:

**Confidencialidade:** A **NOVO CONCEITO** visa garantir que o acesso às informações da companhia, parceiros e de seus clientes sejam obtidos somente por pessoas autorizadas e quando o acesso de fato for necessário;

**Integridade:** A **NOVO CONCEITO** visa garantir a exatidão e a completude das informações e dos métodos de seu processamento, bem como a integridade dos dados de clientes que estejam sob sua responsabilidade.

**Disponibilidade:** A **NOVO CONCEITO** visa garantir que a informação esteja sempre disponível aos profissionais que de fato necessitem o acesso para tal e assegure que os dados estejam acessíveis de acordo com o nível de segurança adequado.

**Rastreabilidade:** A **NOVO CONCEITO** visa garantir a disponibilidade de trilhas de auditoria de informações e meios de processamento, através de registros das transações e alterações realizadas em seu ambiente operacional.

# POLÍTICA EMPRESARIAL



## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023

### 4.2 Aspectos Gerais

- As informações (em formato físico ou lógico) e os ambientes tecnológicos utilizados pelos usuários são de exclusiva propriedade da **NOVO CONCEITO**, não podendo ser interpretado como de uso pessoal;
- As informações de clientes devem ser tratadas de forma ética e sigilosa, de acordo com as diretrizes estabelecidas pela Lei 13.709/2018 - LGPD – Lei Geral de Proteção de dados adotada pela **NOVO CONCEITO** e das leis vigentes;
- As informações de clientes devem ser utilizadas somente para os fins para os quais foram autorizados;
- Todos os integrantes/usuários e colaboradores terceirizados, devem ter ciência de que o uso das informações e dos sistemas de informação podem ser monitorados, sem aviso prévio, e que os registros assim obtidos podem servir de evidência para a aplicação de medidas disciplinares;
- A **NOVO CONCEITO** mantém um compromisso com o cliente em adotar técnicas e meios de segurança mais adequados e disponíveis em relação à segurança dos dados trafegados, processados e/ou armazenados no ambiente operacional da **NOVO CONCEITO**.
- Os integrantes/usuários devem possuir uma identificação única (física e lógica), pessoal e intransferível, que seja capaz de o qualificar como responsável por suas ações;
- Somente profissionais autorizados devem possuir acesso às informações da **NOVO CONCEITO** e de seus clientes;
- Todo processo, sempre que possível, durante seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de uma pessoa ou equipe;
- Os acessos devem sempre obedecer ao critério de menor privilégio, no qual os usuários devem possuir somente as permissões necessárias para a execução de suas atividades;
- Informações confidenciais como senhas e/ou qualquer informação a qual o profissional possua em seu poder durante exercício do seu cargo devem sempre ser mantidas de forma secreta, sendo terminantemente proibido seu compartilhamento;

# POLÍTICA EMPRESARIAL



## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023

- As responsabilidades no que tange a garantia dos pilares da segurança da informação supracitados devem ser amplamente divulgadas, fazendo valer firmemente a aplicação das diretrizes aqui descritas.
- Essa política é apoiada por um conjunto de normativas e procedimentos de segurança da informação estabelecidos pela **NOVO CONCEITO**;
- Não é permitido o compartilhamento de arquivos e pastas da **NOVO CONCEITO** nos computadores e desktops dos colaboradores. Todos os dados deverão ser armazenados exclusivamente na plataforma oferecida pela **NOVO CONCEITO**. Não são permitidos na empresa o compartilhamento de dispositivos móveis tais como pen-drives e outros.
- Todos os dados da empresa deverão ser protegidos através de rotinas sistemáticas de Backup.
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.

### 4.3 Gestão de Acessos e Identidade

Os acessos lógicos dos integrantes/usuários e colaboradores terceirizados devem ser controlados de forma que somente às informações necessárias ao desempenho de suas atividades estejam disponíveis, mediante aprovação formal.

Todo usuário, para acessar os dados da **NOVO CONCEITO**, deverá possuir um login e senha previamente cadastrados pelo DPO.

O DPO fará o cadastramento e informará ao novo usuário qual será a sua primeira senha, a qual deverá, obrigatoriamente, ser alterada imediatamente após o primeiro login e após isso a cada 90 (noventa) dias. As senhas têm critérios mínimos de segurança para que não sejam facilmente copiadas e não possam ser repetidas.

Quando houver necessidade de acesso para usuários externos, sejam eles temporários ou não, a permissão de acesso deverá ser bloqueada tão logo este tenha terminado o seu trabalho, e se houver no futuro nova necessidade de acesso, deverá então ser desbloqueada pelo DPO.

# POLÍTICA EMPRESARIAL



## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023

### 4.4 Gestão de Correio Eletrônico (E-MAIL)

O correio eletrônico fornecido pela **NOVO CONCEITO** é um instrumento de comunicação interna e externa para a realização do negócio. As mensagens devem ser escritas em linguagem profissional, não devem comprometer a imagem da **NOVO CONCEITO**, não podem ser contrárias à legislação vigente e nem aos princípios éticos da **NOVO CONCEITO**.

O uso do correio eletrônico é pessoal e o usuário é responsável por toda mensagem enviada pelo seu endereço. É terminantemente proibido o envio de mensagens que:

- Contenham declarações difamatórias e linguagem ofensiva;
- Possam trazer prejuízos a outras pessoas;
- Sejam hostis e inúteis;
- Sejam relativas a "correntes", de conteúdos pornográficos ou equivalentes;
- Possam prejudicar a imagem da organização;
- Possam prejudicar a imagem de outras empresas;
- Sejam incoerentes com as políticas da **NOVO CONCEITO**.

Para incluir um novo usuário no correio eletrônico, a respectiva Gerência deverá fazer um pedido formal ao DPO, que providenciará a inclusão do mesmo. A utilização do "e-mail" deve ser criteriosa, evitando que o sistema fique congestionado. Em caso de congestionamento no sistema de correio eletrônico, o DPO fará auditorias no servidor de correio e/ou nas estações de trabalho dos usuários, visando identificar o motivo que ocasionou o mesmo.

Não será permitido o uso de e-mails gratuitos (liberados em alguns sites da web).



<p style="text-align: center;"><b>POLÍTICA EMPRESARIAL</b></p> <p style="text-align: center;"><b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b></p>			
<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023



## 4.5 Tratamento da Informação

Para assegurar a proteção adequada às informações da **NOVO CONCEITO**, deve existir um método de classificação e rotulagem da informação de acordo com o grau de confidencialidade e criticidade para os negócios da **NOVO CONCEITO**:

- A classificação deve seguir os seguintes rótulos: Restrita, Confidencial, Interna ou Pública, considerando assim, as necessidades relacionadas ao negócio;
- Todas as informações devem estar adequadamente protegidas em observância às diretrizes de segurança da informação da **NOVO CONCEITO** em todo o seu ciclo de vida, que compreende: geração, manuseio, armazenamento, transporte e descarte;
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada.


## 4.6 Gestão de Riscos, Objetivos e Incidentes de Segurança da Informação

Os riscos devem ser identificados por meio de um processo, estabelecido para Avaliação dos Riscos de Segurança da Informação que afetem o negócio e/ou suas estratégias, alinhados com o contexto do negócio de forma a preservar e proteger adequadamente a **NOVO CONCEITO**.

Os incidentes de segurança da informação devem ser analisados, tratados, registrados, monitorados e reportados ao DPO e/ou dependendo do caso deve reportar também ao **Comitê de Segurança da Informação da NOVO CONCEITO**.

## 4.7 Treinamentos de Conscientização

A **NOVO CONCEITO** deve realizar treinamentos de forma regular e periódica de conscientização em segurança da informação, e as ações devem possuir diferentes formatos e abranger diferentes públicos, podendo ser, mas não se limitando a: Treinamento Presencial ou Regular, EAD e Campanhas de Engenharia Social.

<b>POLÍTICA EMPRESARIAL</b> <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>			
		 <i>Novo Conceito</i>	
<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023


## 4.8 Responsabilidades

De forma geral, cabe a todos os integrantes/usuários, parceiros, e colaboradores terceirizados:

- Cumprir fielmente a Política, as Normas e os Procedimentos de Segurança da Informação da **NOVO CONCEITO**;
- Realizar os treinamentos obrigatórios disponibilizados pela **NOVO CONCEITO**;
- Proteger as informações contra acessos, modificações, destruição ou divulgação não autorizada pela **NOVO CONCEITO**;
- Assegurar que os recursos tecnológicos, as informações e sistemas a sua disposição sejam utilizados apenas para as finalidades aprovadas pela **NOVO CONCEITO**;
- Cumprir as leis e as normas que regulamentam a propriedade intelectual;
- Não discutir assuntos confidenciais de trabalho em ambientes públicos ou em áreas expostas (aviões, transporte, restaurantes, encontros sociais etc.), incluindo a emissão de comentários e opiniões em blogs e redes sociais;
- Comunicar imediatamente ao DPO sobre qualquer descumprimento ou violação desta Política e/ou Normas ou Procedimentos, através do e-mail: [davi@conceitopesquisa.com.br](mailto:davi@conceitopesquisa.com.br), bem como reportar quaisquer incidentes de segurança da informação.

### Cabe à área de Segurança da Informação Corporativa e o DPO.

- Prover ampla divulgação e revisão da Política, Normas e Procedimentos de Segurança da Informação para todos os integrantes/usuários, parceiros e colaboradores terceirizados;
- Promover ações de conscientização sobre Segurança da Informação para todos os integrantes/usuários, parceiros e colaboradores terceirizados.
- Propor e administrar projetos e iniciativas relacionadas ao gerenciamento da segurança da informação da **NOVO CONCEITO**;
- Administrar e monitorar os sistemas e controles aplicados sob gerência da área de segurança da informação da **NOVO CONCEITO**.
- Gerenciar o acesso lógico dos clientes de Cloud;

<b>POLÍTICA EMPRESARIAL</b> <b>POLÍTICA DE SEGURANÇA DA INFORMAÇÃO</b>			
			
<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023

### **Cabe ao Comitê de Conformidade:**

Analisar ocorrências de violações da política de segurança relatadas e suas consequências, quando cabível, respeitadas as atribuições da área de segurança da informação acerca dos indicadores de Riscos de Segurança da Informação.

- Solicitar averiguações em equipamentos e sistemas à área de segurança da informação;
- Direcionar as ocorrências aos Gestores/ Líderes responsáveis para que sejam tomadas as devidas providências.
- Averiguar a severidade do incidente reportado e aplicar as sanções pertinentes.

## 5 AÇÕES DE GERENCIAMENTO

---

A área de segurança da informação (DPO) deve supervisionar o cumprimento desta política, remetendo eventuais casos de descumprimento ao Comitê de Conformidade;

## 6 DISPOSIÇÕES GERAIS

---

Os integrantes são responsáveis por conhecer e entender toda a Documentação Orientadora aplicável a eles. Da mesma forma, os líderes são responsáveis por garantir que todos os seus integrantes entendam e sigam as Documentações Orientadoras aplicáveis da **NOVO CONCEITO**.

Os integrantes que apresentarem dúvidas ou preocupações com relação a esta política, inclusive o escopo, os termos ou as obrigações deste documento, devem entrar em contato com sua respectiva área de conformidade ou com seu líder.

Violações de qualquer Documentação Orientadora da **NOVO CONCEITO** podem resultar em consequências graves para a **NOVO CONCEITO** e para os integrantes envolvidos. Portanto, o **não cumprimento desta Política de Segurança da Informação** implica em falta grave e poderá resultar nas seguintes ações:

# POLÍTICA EMPRESARIAL



## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

<b>Assunto:</b> Política de Segurança da Informação	<b>Projeto:</b> NOVO CONCEITO <b>Tipo documento:</b> PSI	<b>Versão:</b> 1.0	<b>Publicado em:</b> 03/06/2022
<b>Autores:</b> DPO	<b>Classificação:</b> Restrito	<b>Normativa Vinculada:</b> ISO 27001; ISO 27017	<b>Revisão até:</b> 03/06/2023

- Advertência formal;
- Suspensão;
- Rescisão do contrato de prestação de serviço;
- Ação processual civil e/ou criminal.

Esta política entra em vigor na data de sua aprovação.

**03/06/2022**

## 7 APROVAÇÕES

---

Nome / Cargo	Descrição
<i>DPO (Data Protection Officer)</i>	Elaboração
Área de Segurança da informação	Revisão/Recomendação
Comitê de conformidade	Revisão/Recomendação
Comitê de Segurança da informação	Aprovação