

**POLÍTICA DE SEGURANÇA DA  
INFORMAÇÃO**

**RV01 – 29/05/2024**



## POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

As informações da VIATÉCNICA, colaboradores e parceiros são bens que requerem proteção e tratamento de forma ética e sigilosa, de acordo com a legislação vigente e as normas internas da empresa, evitando-se o mau uso, a perda e a exposição indevida. Entende-se por informação, não apenas o que está armazenado nos computadores, redes ou sistemas utilizados pela empresa, mas, também, o que foi impresso ou salvo em mídias digitais e, ainda, o que foi transmitido através de meios eletrônicos ou de conversas em ambientes internos e externos à empresa. O efetivo cumprimento da Política de Segurança da Informação é uma importante ferramenta para combater ameaças a estes ativos da empresa.

Revisão 01

29/05/2024



## Sumário

1. OBJETIVO .....	4
2. DESTINATÁRIOS .....	4
3. DIRETRIZES .....	4
4. PROPRIEDADE DA INFORMAÇÃO .....	5
5. CLASSIFICAÇÃO DA INFORMAÇÃO .....	5
6. UTILIZAÇÃO, GUARDA E DESCARTE DE DOCUMENTOS.....	6
7. BACK-UP .....	6
8. ACESSO CONTROLADO .....	6
9. SEGURANÇA DO AMBIENTE FÍSICO .....	7
10. SEGURANÇA DOS EQUIPAMENTOS .....	7
11. UTILIZAÇÃO GOOGLE DRIVE .....	8
12. UTILIZAÇÃO DOS SISTEMAS CORPORATIVOS .....	8
13. UTILIZAÇÃO DOS EQUIPAMENTOS DE INFORMÁTICA E COMUNICAÇÃO.....	9
14. UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS CORPORATIVOS.....	9
15. ACESSO REMOTO.....	10
16. COMUNICAÇÃO VERBAL DENTRO E FORA DA ORGANIZAÇÃO.....	10
17. RESPONSABILIDADES.....	10
18. TRATAMENTO DE VIOLAÇÕES.....	12



## 1. OBJETIVO

Esta Política de Segurança da Informação é um conjunto de diretrizes que visa conscientizar e orientar os colaboradores, parceiros e clientes da VIATÉCNICA para o uso seguro da informação, garantindo a observância aos princípios inerentes à segurança da informação, quais sejam:

**Integridade:** salvaguarda da exatidão e correção da informação, bem como dos métodos de processamento;

**Confidencialidade:** propriedade que garante que a informação seja acessada somente pelas pessoas ou processos que tenham autorização para tal;

**Disponibilidade:** propriedade da informação estar acessível e utilizável sempre que necessário;

**Autenticidade:** garantia de que seja identificado e registrado o usuário que está enviando ou modificando a informação.

As orientações aqui apresentadas são os princípios fundamentais e representam como a VIATÉCNICA exige que a informação seja utilizada.

## 2. DESTINATÁRIOS

Esta política se aplica a todos os colaboradores da organização certificando-os de que os ambientes, sistemas, computadores e redes da empresa poderão ser monitorados, em qualquer tempo e circunstância.

É obrigação de cada colaborador manter-se atualizado em relação a esta política e aos procedimentos e normas a ela relacionadas, buscando orientação do seu gestor, do comitê de proteção de dados, da área de compliance ou da área de TI sempre que não estiver seguro quanto às diretrizes aqui apresentadas.

## 3. DIRETRIZES

Esta política define as diretrizes para a segurança da informação, visando preservar a integridade, confidencialidade, autenticidade e disponibilidade das informações sob gestão da VIATÉCNICA.



Descreve a conduta considerada adequada para o manuseio, controle e proteção das informações, contra acessos não autorizados, destruição, modificação e divulgação indevida, seja acidental ou intencionalmente.

As condutas aqui estabelecidas estão em total conformidade com a Política de ética e Conduta da VIATÉCNICA.

## 4. PROPRIEDADE DA INFORMAÇÃO

Toda informação produzida, acessada, recebida, manuseada ou armazenada pelos colaboradores, como resultado da atividade profissional, bem como, a reputação, a marca e demais ativos são de propriedade e de direito de uso exclusivos VIATÉCNICA, sendo, portanto, proibidas as cópias, reproduções ou distribuições sem a devida autorização. As exceções devem ser explícitas e formalizadas por meio de e-mail pelo gestor responsável da área ou unidade.

## 5. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade de cada gestor estabelecer critérios relativos ao nível de confidencialidade da informação gerada ou recebido por sua área, de acordo com os critérios a seguir:

- Pública: Informações da empresa com linguagem e formato dedicado à divulgação ao público em geral, sendo de caráter informativo, comercial ou promocional. É destinada ao público externo ou ocorre devido ao cumprimento de legislação;
- Corporativa: Informações cujo conhecimento é de interesse de toda a empresa, podendo ser divulgada para beneficiários, participantes e parceiros;
- Uso Interno: Informações de conhecimento exclusivo dos colaboradores da organização e deve ser divulgada apenas para o público interno;
- Restrita: É toda informação que pode ser acessada somente por colaboradores de áreas previamente definidas.
- Confidencial: É uma informação crítica para os negócios da organização ou de parceiros, devendo haver indicação do nome ou cargo do colaborador responsável. A divulgação não autorizada desta informação pode causar impactos de ordem financeira, de imagem, operacional ou, ainda, sanções administrativas, civis e/ou criminais.



## 6. UTILIZAÇÃO, GUARDA E DESCARTE DE DOCUMENTOS

Documentos que contenham informações classificadas como uso interno, restrita ou confidencial não podem ficar expostos. Documentos que contenham informações classificadas como restrita ou confidencial devem ser acondicionados em armários de acesso controlado.

Nenhuma das informações restritas ou confidenciais podem ser repassadas para terceiros sem consentimento formalizado pela gerência ou diretoria da VIATÉCNICA.

As áreas devem observar a exigência e o prazo legal definido em tabela vigente à época, para manutenção dos documentos produzidos em razão de suas atividades. Decorrido o prazo para armazenamento, os documentos devem ser destruídos antes de descartados, mediante autorização prévia da gerência ou diretoria responsável.

## 7. BACK-UP

Os backups são realizados por sistemas de agendamento e executados, preferencialmente, fora do horário comercial, período em que não há nenhum ou pouco acesso de usuários ou processos automatizados dos sistemas de informática. Os colaboradores responsáveis pela gestão dos sistemas de backup deverão realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida, sugestões de melhorias, entre outros.

## 8. ACESSO CONTROLADO

Para cada colaborador da VIATÉCNICA é fornecido logins de acesso e senhas, os quais, não poderão ser compartilhados, divulgados ou transferidos a outra pessoa. O colaborador é responsável por todas as atividades desenvolvidas por meio de seus logins de acesso pessoal. É vedada, a qualquer colaborador, a utilização de login de acesso pessoal de outro colaborador mesmo quando cedida por este. É de responsabilidade de cada colaborador da organização a guarda dos logins de acessos que lhe forem designados.

Se existir login de uso compartilhado por mais de um colaborador, a responsabilidade perante a organização e a legislação (cível e criminal) será dos colaboradores que dele se utilizarem. A concessão de acessos deverá seguir o critério de menor privilégio, no qual os colaboradores tenham acesso apenas às informações imprescindíveis para o



pleno desempenho de suas atividades. Cada gerente de área deverá solicitar à equipe de TI inclusões, alterações ou exclusões de acesso a usuários, definindo os 7 serviços que deverão ser incluídos, alterados ou excluídos e justificando quanto à necessidade da solicitação. Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários. Portanto, por ocasião do desligamento de qualquer colaborador, a Equipe de TI deverá ser comunicada para providenciar o imediato cancelamento de todas as suas senhas de acesso a equipamentos e sistemas corporativos, bem como de seu e-mail, sendo esse comunicado previamente pela gerência responsável pelo colaborador desligado ou transferido de área.

## 9. SEGURANÇA DO AMBIENTE FÍSICO

É vedado o acesso de pessoas não autorizadas. O acesso de visitantes às áreas internas da VIATÉCNICA deverá ser supervisionado pelo gestor da área responsável. As áreas de acesso restrito, somente podem ser acessadas por colaboradores devidamente autorizados.

O acesso às dependências da organização com quaisquer equipamentos de gravação, fotografia, vídeo, som ou outro tipo de equipamento similar, para fins de gravação dos ambientes de trabalho, somente poderá ser realizado a partir de autorização da gerência ou diretoria e mediante supervisão. Não é permitido aos colaboradores tirar fotos, gravar, filmar, publicar e / ou compartilhar imagens dos ambientes internos da VIATÉCNICA que possam comprometer a segurança dos demais colaboradores, o sigilo das informações, impactar negativamente a imagem da VIATÉCNICA, outros colaboradores, clientes, parceiros e/ou visitantes.

## 10. SEGURANÇA DOS EQUIPAMENTOS

É proibido todo procedimento de manutenção física ou lógica, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento da área de TI. Os sistemas e computadores devem ter versões de software antivírus instalados, ativados e atualizados permanentemente. Em caso de suspeita de incidência de vírus ou problemas de funcionalidade de hardware ou software, o colaborador deverá acionar a área de TI. Os colaboradores deverão proteger o acesso a seus computadores por meio de tela de bloqueio a ser liberada mediante senha, quando os mesmos não estiverem em uso. Ao final do expediente de trabalho, o computador deverá ser desligado



## 11. UTILIZAÇÃO GOOGLE DRIVE

A VIATÉCNICA possui uma rede integrada de computadores com servidores de autenticação de usuários e impressão, e um computador e/ou notebook para cada colaborador alocado na matriz, além de acesso ao drive compartilhado do Google para atender colaboradores da matriz e obras. O acesso ao drive compartilhado do Google através de autenticação via conta de e-mail corporativo de cada colaborador.

O colaborador é responsável pelas atividades realizadas por intermédio de sua conta de usuário e senhas de acesso. Os colaboradores da VIATÉCNICA não deverão obter ou disponibilizar material sem a licença adequada. O usuário é responsável pela própria e devida autenticação nos sistemas de redes e acesso ao drive compartilhado do Google disponibilizados pela VIATÉCNICA, não podendo fornecer e / ou compartilhar seu usuário, senha e / ou acessar com outros usuários. O usuário está comprometido a utilizar o drive compartilhado do Google para uso exclusivo de atividades relacionadas ao setor no qual o usuário pertence.

É vedada a utilização de proxies que permitam o tráfego de informações a redes privadas externas. Os usuários devem administrar suas pastas, excluindo arquivos desnecessários. Material sexualmente explícito ou contrário à legislação brasileira não podem ser expostos, armazenados, distribuídos, editados ou gravados, através do uso dos recursos computacionais da rede corporativa da empresa. Não é permitida a gravação de arquivos particulares (músicas, filmes, fotos etc..) nos drivers de rede e drive do Google. Caso identificada a existência desses arquivos, eles poderão ser excluídos definitivamente, sem prévia comunicação.

## 12. UTILIZAÇÃO DOS SISTEMAS CORPORATIVOS

Os sistemas corporativos são os sistemas utilizados na gestão VIATÉCNICA, os quais buscam trazer maior organização para as informações, abrangendo todos os segmentos da administração, permitindo o gerenciamento isolado de cada parte e a interligação desta com o todo, produzindo relatórios analíticos, sintéticos e estatísticos.

É expressamente proibida a divulgação e / ou o compartilhamento indevido das informações contidas nos sistemas corporativos da VIATÉCNICA. Todos os usuários dos ativos de informação de propriedade da VIATÉCNICA, ao utilizarem esse serviço, deverão fazê-lo no estrito interesse do mesmo, mantendo conduta profissional.

O acesso às informações contidas nos sistemas corporativos deve ser efetuado sempre através de identificação segura (login e senha). Para cada usuário devem ser atribuídas permissões específicas, por módulo e/ou operação. A concessão de





acesso às bases de dados para prestadores de serviço e colaboradores deverá sempre seguir o critério do menor privilégio possível.

### **13. UTILIZAÇÃO DOS EQUIPAMENTOS DE INFORMÁTICA E COMUNICAÇÃO**

Os equipamentos de informática e de comunicação são utilizados pelos colaboradores da empresa para a realização das atividades profissionais. Excepcionalmente, o uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos sistemas e serviços. A VIATÉCNICA, por meio de sua área de TI, poderá registrar todo e qualquer uso dos sistemas e serviços, visando garantir a disponibilidade e a segurança das informações utilizadas.

A responsabilidade em relação à segurança da informação será comunicada na fase de contratação dos colaboradores, os quais deverão assinar um termo de responsabilidade dos equipamentos e confidencialidade das informações. Os acessos ao drive compartilhado do Google possuem rastreabilidade de todas as atividades executadas por cada colaborador, sendo assim é de responsabilidade de cada colaborador zelar pelos seus respectivos acessos.

### **14. UTILIZAÇÃO DE DISPOSITIVOS MÓVEIS CORPORATIVOS**

É expressamente proibida a divulgação e/ou o compartilhamento indevido de informações de uso interno, restritas ou confidenciais por meio de dispositivos móveis corporativos. O usuário deve utilizar os dispositivos móveis corporativos de forma adequada e diligente, de forma a prevenir ações que possam danificar, inutilizar, sobrecarregar ou deteriorar os recursos tecnológicos, bem como os documentos e arquivos de qualquer tipo, de seu uso ou de uso de terceiros.

O usuário é pessoalmente responsável por todas as atividades realizadas por intermédio de dispositivos móveis corporativos, tanto por sua guarda, quanto pelos conteúdos neles instalados. Não é permitida a alteração da configuração dos sistemas operacionais dos equipamentos, em especial, os referentes à segurança e à geração de logs, sem a devida comunicação e a autorização da área responsável e sem a condução, auxílio ou presença de um colaborador da área de TI.

É responsabilidade do colaborador, no caso de furto ou roubo de um dispositivo móvel fornecido pela VIATÉCNICA, notificar imediatamente seu gestor e a área de TI. Também deverá, assim que possível, registrar um Boletim de Ocorrência na



Delegacia de Furtos de Roubos (BO). O colaborador deverá estar ciente de que o uso indevido do dispositivo móvel caracteriza a assunção de todos os riscos da sua má utilização, sendo o único responsável por quaisquer danos, diretos ou indiretos, presentes ou futuros, que venha causar a organização e/ou a terceiros. Em caso de desligamento, o colaborador deve realizar imediata devolução de seus dispositivos móveis à área de TI e assinar o termo de devolução do equipamento.

## **15. ACESSO REMOTO**

O acesso a redes remotas permite ao usuário acessar, utilizar e executar aplicações e sistemas operacionais disponibilizados naquele ambiente, desde que tenham acesso autorizado para isto.

A boa utilização destes serviços é de responsabilidade de cada usuário, os que utilizam o drive compartilhado da VIATÉCNICA e/ou terceiros que utilizam serviços de acesso remoto. Cabe ressaltar que os serviços estão disponibilizados para o uso estritamente profissional e de interesse da organização. O usuário somente poderá realizar as atividades em período estipulado pela VIATÉCNICA e devidamente autorizado por seu gestor.

## **16. COMUNICAÇÃO VERBAL DENTRO E FORA DA ORGANIZAÇÃO**

Somente os colaboradores que estão devidamente autorizados a falar em nome VIATÉCNICA, para os meios de comunicação, podem fazê-lo em nome da organização.

A fim de evitar exposição desnecessária da VIATÉCNICA, os colaboradores não devem tratar de assuntos internos em locais públicos ou dentro das instalações físicas da organização, quando próximos a visitantes ou terceiros.

## **17. RESPONSABILIDADES**

A correta utilização dos recursos disponibilizados é dever de todos os colaboradores da organização, sendo que o uso indevido, negligente ou imprudente será responsabilizado, conforme normativos internos e legais. A VIATÉCNICA reserva-se o direito de analisar dados e evidências, a fim de obter provas, que possam ser utilizadas nos processos investigatórios, bem como, adotar as medidas legais cabíveis.

## **17.1. TODOS OS COLABORADORES**

- Conhecer e cumprir a presente política;
- Assinar termo de ciência e responsabilidade sobre a política declarando ter conhecimento de suas responsabilidades;
- Buscar orientação em caso de dúvidas relacionadas à segurança da informação;
- Fiscalizar e orientar os parceiros e clientes da organização quanto às diretrizes desta política;
- Observar os princípios constantes na Política de Ética e Conduta;
- Comunicar imediatamente quando do descumprimento ou violação desta política, conforme diretrizes.

## **17.2. COMITÊ DE PROTEÇÃO DE DADOS**

- Determinar a adoção de medidas necessárias para o cumprimento da política;
- Implantar e implementar a presente política;
- Orientar e informar aos colaboradores as práticas necessárias à segurança da informação; d) Receber o report de todo e qualquer usuário e/ou área para tratar de assuntos pertinentes à segurança da informação de que trata este instrumento;
- Promover juntamente com a área de TI e os gestores dos processos a segregação de acessos necessários aos sistemas da VIATECNICA, evitando conflitos de interesse e adotando perfis de acesso;
- Receber e tratar as notificações dos casos de violação das diretrizes de segurança expostas neste instrumento;
- Realizar testes e atualizações nos diversos acessos aos recursos de TI

## **17.3. DIRETORIA EXECUTIVA**

- Promover a política de segurança e o cumprimento das normas aqui presentes.

## **17.4. GESTORES**

- Fazer cumprir as normas aqui presentes;
- Assegurar que as equipes possuam acesso e conhecimento desta política;
- Promover juntamente com a área de TI e o comitê de proteção de dados a segregação de acessos necessários aos sistemas da VIATÉCNICA, evitando conflitos de interesse e adotando perfis de acesso.

## 18. TRATAMENTO DE VIOLAÇÕES

Os casos de violação das diretrizes de segurança expostas neste instrumento poderão ser notificados, conforme disposto abaixo:

1. Por meio dos nossos canais de atendimento. Quando for uma ocorrência interna.
2. Ao gestor de cada área;
3. O usuário infrator estará passível das seguintes penalidades imediatas, sem prévio aviso;
4. Descredenciamento da senha de acesso à Internet;
5. Cancelamento da conta de e-mail;
6. Cancelamento do acesso aos sistemas corporativos;
7. Desativação do ponto de rede do usuário. O responsável por receber a notificação da transgressão deverá acionar imediatamente o comitê de proteção de dados, o qual fará a comunicação ao usuário infrator e à gerência ou diretoria correspondente, para aplicação das penalidades previstas na Política de Ética e Conduta da VIATÉCNICA e na legislação vigente no Brasil.

