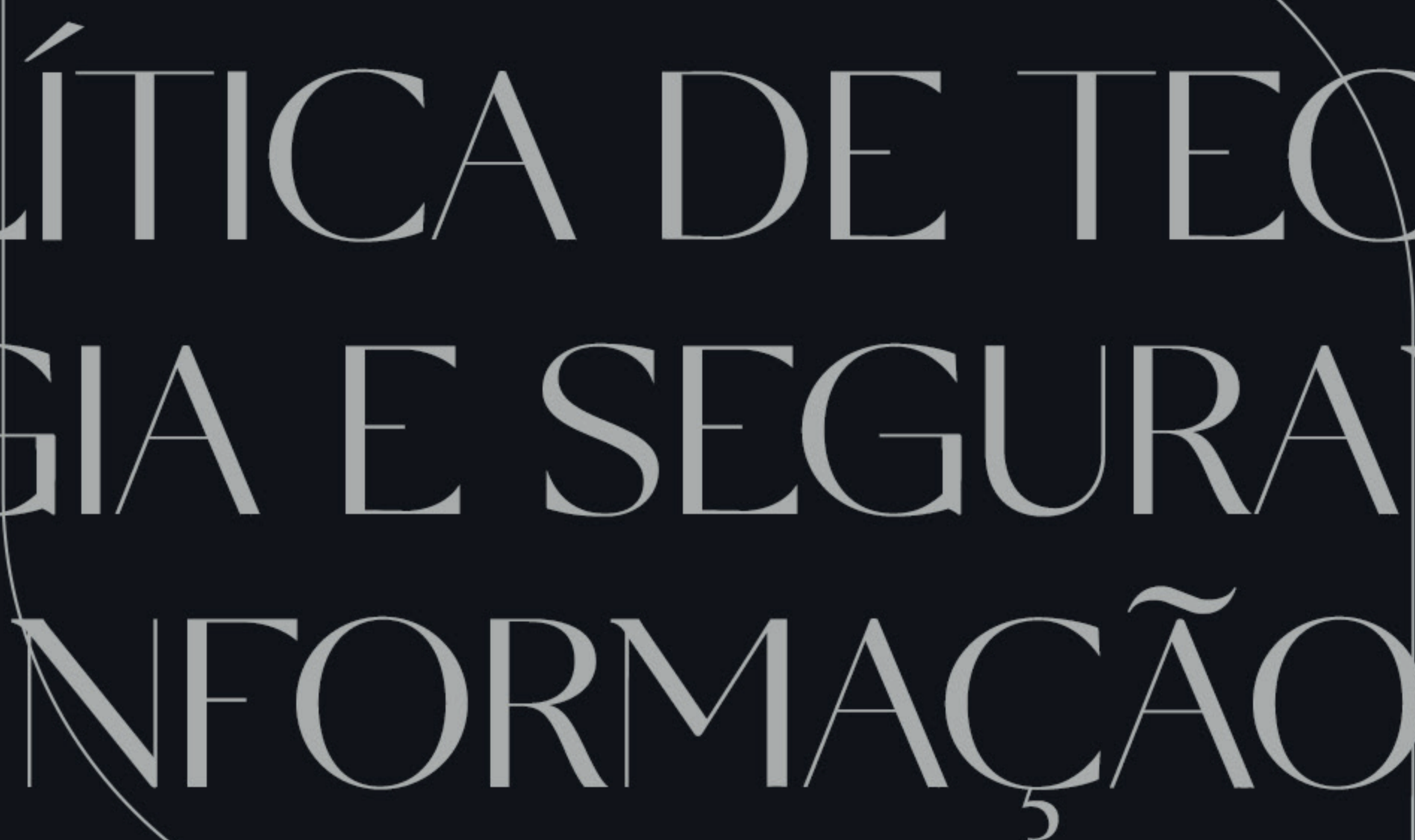


POLÍTICA DE TECNO
LOGIA E SEGURANÇA
DA INFORMAÇÃO





tif

1

Objetivo

1. Objetivo

Estabelecer as diretrizes que orientam a utilização, aquisição, desenvolvimento e gestão de recursos de tecnologia da informação, em consonância com as boas práticas de mercado e visando garantir a integralidade, confidencialidade e legalidade das informações necessárias para a realização das atividades da Tif.



tif

2

Aplicação



2. Aplicação

A Política de Segurança da Informação é um documento que registra os princípios e as diretrizes de segurança adotado pela Tif Comunicação, aplicando-se a todos os funcionários, prestadores de serviços, sistemas e serviços, incluindo trabalhos executados externamente ou por terceiros, que utilizem o ambiente de processamento corporativo, ou acesso a informações pertencentes à Tif.

Assim, é dever de todos dentro da Tif considerar a informação como sendo um bem da empresa, sendo um dos recursos para a realização dos trabalhos, devendo sempre ser tratada de maneira muito profissional.



3

tif

Definições

3. Definições

Ambiente Corporativo - O ambiente corporativo refere-se à infraestrutura de recursos computacionais composto por comunicação, armazenamento de dados, segurança da informação e processamento de dados.

Gestores: CEO, Diretores e Heads de Criação, Atendimento e Mídia, Diretor de Operações e Gerente Administrativo e Financeiro.

Aplicativos de Uso Geral - Programas de computador que auxiliam e automatizam vários tipos de tarefas e rotinas de trabalho. Exemplos: editores de texto, editores de apresentação de slides, planilhas eletrônicas, etc.

Backup - Cópia de segurança - termo utilizado em informática para indicar a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento.

Informação Interna: é toda informação que só pode ser acessada por funcionários da Tif. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da empresa ou de um cliente.

Aplicativos Utilitários - Programas de computador que auxiliam nas diversas tarefas ligadas ao gerenciamento, monitoramento, otimização e manutenção do computador.

Informação Confidencial: é toda informação de caráter sigiloso, que pode ser acessada por funcionários e clientes, nos termos definidos por esta política, pelo Código de Ética e demais normas que integram nossa Política de Compliance e cuja divulgação não autorizada pode causar impacto (financeiro, de imagem ou operacional) ao negócio da Tif ou ao negócio do cliente.

Recursos de Tecnologia da Informação:

quaisquer equipamentos ou dispositivos que utilizem tecnologia da informação, bem como quaisquer recursos ou informações que sejam acessíveis através desses equipamentos ou dispositivos tecnológicos, tais como impressoras, sistemas, programas, softwares, acessos à rede local e suas pastas de compartilhamento, internet e outros tipos de conexão, armazenamento e/ou processamento de dados.

Informação Pública:

é toda informação que pode ser acessada por clientes, fornecedores, prestadores de serviços e público em geral.

**TI – Tecnologia da Informação:**

conjunto de todas as atividades e soluções providas por recursos computacionais que visam permitir a obtenção, o armazenamento, o acesso, o gerenciamento e o uso das informações.

Usuário Final

- Cliente ou consumidor de software e hardware que os utiliza para desempenhar suas atividades profissionais.

Usuário de Suporte

- Colaborador (do quadro próprio ou terceirizado) que atua na gestão e na manutenção de recursos de tecnologia da informação.



4.tif

Descrição

4. Descrição

A presente norma dispõe sobre a gestão do ambiente de Segurança da Informação da Tif, a definição do perfil da tecnologia a ser utilizada e sua aplicação, bem como o processo a ser seguido na introdução de novos recursos de TI.

4.1. Admissão/Demissão de colaboradores e estagiários

Os gestores de cada departamento deverão informar ao setor Administrativo, toda e qualquer movimentação de colaboradores temporários ou estagiários, e admissão e demissão de colaboradores, bem como prestadores de serviços - pessoas físicas ou jurídicas - para que estes possam ser cadastrados ou excluídos no sistema da Tif. Isto inclui o fornecimento de sua senha (“password”) e registro do seu nome como usuário no sistema (“user-id”), pelo setor Administrativo, para utilização do sistema e do programa “Publi”, e a criação da conta de e-mail.

Cabe ao setor solicitante da contratação a comunicação ao setor Administrativo sobre as rotinas a que o novo contratado terá direito de acesso.

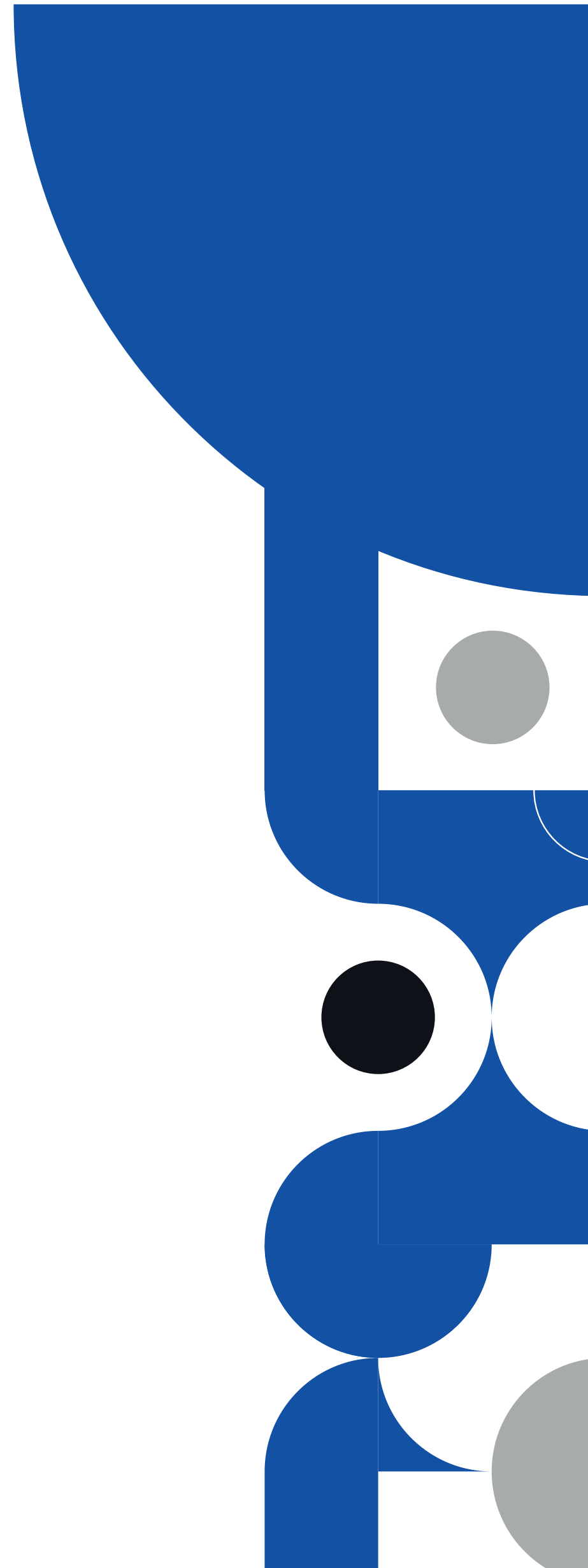
O Serviço de Informática fará o cadastramento e informará ao novo usuário qual será a sua primeira senha. Por razões de segurança, a Tif recomenda que o usuário altere sua senha a cada 60 (sessenta dias) por razões de segurança.

Ressaltamos que o cuidado com a senha e a adoção das recomendações de segurança é de inteira responsabilidade do usuário, o qual poderá responder por eventuais incidentes e vazamentos de dados.

No caso de demissão, o setor Administrativo deverá comunicar o fato o mais rapidamente possível à Informática, para que o colaborador desligado seja prontamente excluído dos acessos concedidos pela Tif, especialmente do e-mail, Teams, Publi, Meta, Google, Dashboard de clientes e Rede/Next.

No momento da contratação, cabe ao setor Administrativo dar conhecimento e obter as devidas assinaturas de concordância dos novos colaboradores em relação à Política de Segurança da Informação da Tif.

Nenhum funcionário, estagiário ou temporário, bem como prestadores de serviços - pessoas físicas ou jurídicas - poderá ser contratado, sem ter expressamente concordado com esta política.



4.2. Segurança e Integridade de dados

O gerenciamento dos servidores, sistemas e banco de dados da Tif é responsabilidade exclusiva do Setor Administrativo, através do Serviço de Informática, assim como a manutenção, alteração e atualização de equipamentos e programas.

4.3. Unidades de rede e de armazenamento em “nuvem”

Os espaços de armazenamento de rede são destinados exclusivamente para uso nas atividades relativas ao negócio da Tif e serão incluídos na rotina diária de backup da Informática.

A empresa se reserva no direito de acessá-los e monitorá-los quando julgar necessário e a qualquer tempo. Para arquivos e trabalhos armazenados em “nuvem”, serão disponibilizados acessos para os colaboradores envolvidos no trabalho.

Todos os acessos a arquivos armazenados em “nuvem” são destinados exclusivamente para uso nas atividades relativas ao negócio da Tif, sendo terminantemente proibidos os acessos não autorizados, utilizações para outros fins, bem como compartilhamentos com terceiros não autorizados expressamente pela Tif.

Em qualquer hipótese, todo o colaborador que venha a ser desligado da empresa, bem como prestadores de serviços - pessoas físicas ou jurídicas - que tenham seus contratos rescindidos, terão seus acessos imediatamente interrompidos.

Ainda que essa interrupção não seja implementada de imediato, os colaboradores ficam cientes de que, após o seu desligamento, estão expressamente proibidos de acessar arquivos, pastas, diretórios e programas da empresa, sejam eles localizados em hardwares, ambientes de rede ou em “nuvem”, podendo eventual acesso ser configurado como invasão e/ou quebra de sigilo, com as conseqüentes repercussões de ordem legal, inclusive criminal.

Caso o colaborador desligado necessite de algum arquivo que entenda ter direito, deverá realizar solicitação formal ao Setor Administrativo, que a repassará à Diretoria de Operações para análise da questão.

4.4. Uso de e-mail corporativo

O e-mail corporativo fornecido pela Tif é um instrumento de comunicação interna e externa para a realização do negócio da Tif. As caixas de e-mail disponibilizadas pela Tif são de sua propriedade, podendo a empresa acessá-las e monitorá-las a qualquer tempo quando julgar necessário. As mensagens devem ser escritas em linguagem profissional, seguindo os princípios estabelecidos no Código de Ética e obedecendo a legislação vigente.

O uso do e-mail é pessoal e intransferível, sendo o usuário responsável por toda mensagem enviada pelo seu endereço.

É terminantemente proibido o envio de mensagens que:

- Que contenham conteúdos pornográficos, de conotação sexual ou equivalentes;
- Sejam incoerentes com o Código de Ética e as políticas adotadas pela Tif;
- Contenham declarações difamatórias e linguagem ofensiva;
- Possam prejudicar a imagem de clientes ou fornecedores;
- Possam prejudicar a imagem da organização;
- Sejam relativas a “correntes”;
- Sejam hostis e inúteis.

Para incluir um novo usuário de e-mail, o respectivo gestor deverá pedir ao Setor de Administrativo, que providenciará a inclusão.

4.5. Monitoramento e acesso à internet

O acesso à Internet na Tif é destinado a todos os colaboradores para execução de suas atividades de trabalho. A Tif poderá se utilizar de mecanismos para bloqueio automático de acesso a conteúdo e serviços da Internet, que contenham informações alheias aos interesses da empresa. A Tif também poderá se utilizar de aplicativos de monitoramento e controle de acessos de colaboradores a sites de Internet. Informações como o endereço do site, a quantidade de dados trafegados e o tempo de acesso, poderão ser gravadas e disponibilizadas para consulta e geração de relatórios a pedido dos Diretores.

Os usuários devem se assegurar de que não estão executando ações que possam infringir direitos autorais, marcas, licença de uso ou patentes de terceiros. Quando navegando na Internet, é proibida a visualização, transferência (downloads), cópia ou qualquer outro tipo de acesso a sites:

- Que permitam a transferência (downloads) de arquivos e/ou programas ilegais;
- Que menosprezem, depreciem ou incitem o preconceito a classes sociais;
- Que possibilitem a distribuição de informações de nível “Confidencial”;
- De conteúdo pornográfico ou relacionados a sexo;
- Que defendam atividades ilegais.

4.6. Dispositivos de armazenamento de dados

A Tif não se responsabiliza por dados particulares armazenados em computadores, periféricos e servidores de arquivos de sua responsabilidade. Os espaços de armazenamento destes equipamentos são destinados exclusivamente para uso nas atividades relativas ao negócio da empresa.

A Tif se reserva o direito de acessá-los e monitorá-los quando julgar necessário e a qualquer tempo.

O uso de dispositivos particulares que permitam armazenamento de dados como pen-drives, hd (hard disk) externos e cartões de memória são proibidos, salvo em situações específicas, mediante autorização da diretoria.

4.7. Necessidades de novos sistemas, aplicativos ou equipamentos

Qualquer necessidade de novos programas (“softwares”) ou de novos equipamentos de informática (“hardware”) deverá ser discutida com o gestor de cada setor.

Não é permitido o download, a compra ou o desenvolvimento de “softwares” ou “hardwares” diretamente pelos colaboradores.

4.8. Programas ilegais

É proibido download, a instalação e o uso de programas ilegais (“piratas”) na Tif. Os usuários não podem, em hipótese alguma, instalar este tipo de “software” nos equipamentos da empresa.

Periodicamente, o Serviço de Informática poderá fazer verificações nos dados dos servidores e nos computadores dos colaboradores, visando garantir a correta aplicação desta diretriz.

4.9. Uso de antivírus

Todas as estações de trabalho devem ter um antivírus instalado. A atualização do antivírus será automática.

Todos os arquivos em mídia proveniente de entidade externa a Tif, arquivos recebidos ou obtidos da Internet, devem ser verificados por programa antivírus.

O usuário não pode em hipótese alguma, desabilitar o programa antivírus instalado nas estações de trabalho.

4.9.1. Uso de Notebook/ Laptop ou Tablets de propriedade da Tif

Os usuários que tiverem direito ao uso de notebook, laptop, tablets ou qualquer outro equipamento computacional, de propriedade da Tif, devem estar cientes de que:

Os recursos de tecnologia da informação, disponibilizados para os usuários, têm como objetivo a realização de atividades profissionais; a proteção do recurso computacional de uso individual é de responsabilidade do próprio usuário; é de responsabilidade de cada usuário assegurar a integridade do equipamento, a confidencialidade e disponibilidade da informação contida no mesmo; o usuário não deve alterar a configuração do equipamento recebido.

Fora do ambiente de trabalho, os usuários devem manter os equipamentos sempre sob sua vigilância e não acessar informações confidenciais em locais públicos.

Em caso de dano, furto ou extravio do equipamento, é obrigatório o aviso imediato à Tif e registrar a ocorrência em delegacia de polícia, encaminhando cópia ao gestor para que tome todas as medidas de segurança cabíveis.

Se o equipamento for danificado ou inutilizado por emprego inadequado, mau uso, negligência ou extravio, a Tif solicitará ressarcimento do valor do conserto ou de um equipamento da mesma marca ou equivalente, de acordo com a situação.

Finalizado os serviços, ou na hipótese de rescisão do contrato de trabalho ou de prestação de serviços, o equipamento deverá ser devolvido completo e em perfeito estado de conservação, considerando-se o tempo de uso.

4.10. Responsabilidades dos Gestores

Os gestores são responsáveis pelas definições dos direitos de acesso de seus colaboradores aos sistemas e informações da Tif, cabendo a eles verificarem se eles estão acessando exatamente as rotinas compatíveis com as suas respectivas funções, usando e conservando adequadamente os equipamentos, conforme estabelecido nesta política.



tif

5

Violações

5. Violações

A violação desta Política de Segurança é qualquer ato que:

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

O não cumprimento desta Política de Segurança da Informação implica em falta grave e poderá resultar nas seguintes ações: advertência formal, suspensão, rescisão do contrato de trabalho, entre outras ações disciplinares, sem prejuízo da responsabilização civil e/ou criminal.

Canais de Compliance Tif:

✉ compliance@tif.com.br

🌐 tif.com.br/compliance