
Tamandaré
Technology

A tecnologia transformou a execução das atividades profissionais na Sociedade Digital. Antes havia fronteiras físicas, as informações eram verbalizadas e não chegavam instantaneamente ao seu destino, além de estarem sempre materializadas em suportes físicos.

Na **Sociedade Digital** em que a mobilidade e as mídias sociais estão presentes diariamente na rotina das pessoas, não há mais fronteiras, a informação é compartilhada de maneira global, de forma instantânea e reproduzida inúmeras vezes. **Tudo está documentado e pode ser visto por qualquer pessoa!**

Diante desse cenário, em que os dados estão mais acessíveis e a tecnologia possibilita sua rápida transmissão e propagação, a **Segurança é Digital** deve alcançar além do conteúdo escrito no papel ou gravado em um dispositivo informático, abrangendo, principalmente, **a reputação, a imagem e o conhecimento da empresa** por meio de uma compreensão holística de segurança, onde qualquer fator pode comprometer todo o sistema, ainda que de forma colateral.

Surge uma nova realidade: **A segurança deve acompanhar a informação, independente do lugar onde ela esteja.**

Como já indicado, **a informação pode ser registrada de diversas formas e compartilhadas por qualquer um e a qualquer tempo** na Sociedade Digital, das mais variadas formas, desde a publicação de um vídeo, envio de torpedo ou uso de mídias sociais.

Por isso, o cuidado com os dados da **TAMANDARÉ** é extremamente relevante e **exige atenção**, já que os impactos decorrentes da sua utilização indevida podem afetar negativamente o patrimônio, a imagem e a reputação da empresa de maneira irrecuperável. **Os controles exigidos para se perpetuar a Segurança Digital demandam mudança de postura e maior atenção com tudo o que se veicula e se manuseia, especialmente ativos de tecnologia da informação e comunicação.**

Entretanto, muitas vezes, nos esquecemos de proteger adequadamente o conteúdo corporativo, seja pela pressa ou pela sensação de segurança que a tecnologia oferece. Assim, esta **Cartilha** tem como objetivo orientar sobre

as **melhores práticas e hábitos que precisam ser introduzidos na rotina diária de todos os colaboradores e prestadores de serviço**, para que possamos evoluir e crescer com devidamente autorizados;

•AUTENTICIDADE: garantia de que quem criou ou modificou a informação é quem se diz ser;

•LEGALIDADE: conformidade legal do tratamento da informação em todas as etapas de seu ciclo de vida. **TAMANDARÉ** possui uma **Política de Segurança da Informação (PSI)**.

Nela você pode entender mais sobre as intenções da direção da **TAMANDARÉ** quanto à proteção de informações e qual o seu papel para o sucesso da empresa.

Conheça, cumpra, mantenha-se atualizado e compartilhe com seus colegas!
Para acessá-la acesse a pasta da rede Geral através do caminho: O:\Normas Internas Entretanto, a proteção da informação não é uma tarefa simples, pois o sucesso depende da **perfeita sinergia entre tecnologias, processos e pessoas**, sendo fundamental o esforço e a contribuição de todos no que se refere ao comportamento e cumprimento orientações previstas nesta **Cartilha** e nos demais documentos da **TAMANDARÉ**!

A Segurança da Informação exige disseminação de condutas seguras por todos os colaboradores e prestadores de serviço, todo o tempo, de forma que os hábitos de segurança se incorporem no dia-a-dia de cada um.

Todos os nossos colaboradores e prestadores de serviço, em qualquer nível hierárquico, são fundamentais para o sucesso das iniciativas de **Segurança da Informação Na TAMANDARÉ**, principalmente como utilizam as informações e os ativos de tecnologia da informação e comunicação que lhe são disponibilizados.

A **TAMANDARÉ** é a **proprietária** de todos os ativos intangíveis, das informações e de todas as ferramentas tecnológicas fornecidas para o desempenho de atividades profissionais, incluindo os dispositivos de mobilidade e todo o perímetro lógico e físico.

Por isso, só podem ser utilizados para o **estrito cumprimento das atividades profissionais** ligadas às funções contratadas pela **TAMANDARÉ**, atendendo à obrigação de **sigilo profissional e preservando a classificação da informação indicada**.

Sustentabilidade e atendendo aos requisitos que nos são exigidos de governança corporativa e segurança da informação.

Assim, todos os colaboradores e prestadores de serviço são responsáveis por zelar pela **proteção das informações**, dos **ativos intangíveis** (ex. a reputação, imagem, marca e conhecimento da empresa) e dos **ativos de tecnologia da informação e comunicação da TAMANDARÉ**, evitando a exposição desnecessária dos dados corporativos na internet, especialmente nas mídias sociais, e aplicando todas as recomendações desta **Cartilha de Segurança da Informação** e dos demais documentos relacionados à segurança da informação **todo o tempo**!

É fundamental, da mesma forma, manter-se sempre atualizado e ficar atento às orientações apresentadas para não praticar ações que possam prejudicar sua vida profissional tanto no presente quanto no futuro, além de ter consciência de que **os esforços de cada um impactam em toda a empresa**!

A informação é um ativo critico para as atividades da **TAMANDARÉ** e como tal deve ser preservada com controles e ferramentas proporcionais ao impacto decorrente da sua geração, alteração, destruição ou veiculação inadequadas, sejam elas acidentais ou intencionais.

Assim, **a Segurança da Informação é a proteção das informações corporativas contra diversas ameaças**. Visa garantir a continuidade dos processos de negócio, minimizar os eventuais danos, inclusive a terceiros, além de maximizar o retorno de investimentos e oportunidades, protegendo a reputação da **TAMANDARÉ** e prevenindo eventos indesejados.

Para isso, devemos ter sempre em mente que o objetivo maior da **Segurança da Informação** é garantir a manutenção dos seguintes atributos da informação:

• DISPONIBILIDADE: garantia de que a informação e os ativos de tecnologia da informação e comunicação estejam oportunamente acessíveis sempre que necessários;

• INTEGRIDADE: garantia de que a informação seja protegida contra alterações ou exclusões indevidas, intencionais ou acidentais, devendo ser mantida em seu estado original ou de última modificação válida;

• CONFIDENCIALIDADE: garantia de que a informação seja acessível apenas aos indivíduos que possuem as devidas permissões e processos automáticos

Evite abrir arquivos recebidos por correio eletrônico, comunicadores instantâneos, baixados da internet ou por dispositivos removíveis **sem examiná-los por software de detecção de vírus homologado pela TAMANDARÉ**.

Nem tudo que está na internet é publico. Por isso, recomendamos que não seja instalado ou efetuado o download de quaisquer arquivos ou softwares de origem duvidosa, pirata ou que não tenham sido autorizados pela **TAMANDARÉ**, mesmo que a finalidade seja para aumentar a produtividade ou melhorar a execução das atividades profissionais.

Caso necessário, solicite autorização ao superior hierárquico ou diretamente a Área de Tecnologia da Informação que efetuará a liberação, quando pertinente.

Normalmente, esses conteúdos estão infectados por algum tipo de programa malicioso que pode expor as informações e os recursos às ameaças e riscos à segurança das informações e da infraestrutura tecnológica da empresa.

PIRATARIA É CRIME!

Utilize somente hardwares e softwares autorizados previamente pela **TAMANDARÉ**.

Código Penal:

Art. 184 - Violar direitos de autor e os que lhe são conexos:

Pena - detenção, de 3 (três) meses a 1 (um) ano, ou multa.

Respeite os Direitos Autorais!

Verifique sempre a permissão dos conteúdos baixados e/ou utilizados da internet e cite sempre a fonte e a autoria.

O respeito ao sigilo de uma informação corporativa é essencial para o crescimento sustentável do negócio. **A informação é a base e a estrutura de qualquer empresa**.

Se indevidamente revelada, pode acarretar prejuízos negativos de ordem incalculável.

Para garantir a proteção adequada da informação de acordo com o seu nível de criticidade para o negócio, recomendamos que todas as informações corporativas sejam rotuladas e classificadas no momento da sua geração ou obtenção, de forma a permitir fácil identificação pelos demais colaboradores e prestadores de serviço e o correto manuseio durante todo o seu ciclo de vida.

Além disso, a utilização das marcas, identidade visual e sinais distintivos da **TAMANDARÉ** em qualquer forma ou mídia, principalmente na internet e nas mídias sociais necessitam de autorização prévia e específica, a menos que exista permissão já existente da empresa, conferida de modo expresso.

O mau uso das ferramentas corporativas, o desrespeito aos regulamentos internos e a revelação indevida de informações da LTA-RH podem gerar demissão por justa causa:

Consolidação das Leis Trabalhistas:

Art. 482 – Constituem justa causa para rescisão do contrato de trabalho pelo empregador (...):

b) incontinência de conduta ou mau procedimento; (...);

e) desídia (desleixo) no desempenho das respectivas funções; (...);

g) violação de segredo da empresa; (...);

j) ato lesivo da honra ou da boa fama praticado no serviço contra qualquer pessoa, ou ofensas físicas, nas mesmas condições, salvo em caso de legítima defesa, própria ou de outrem;

k) ato lesivo da honra ou da boa fama ou ofensas físicas praticadas contra o empregador e superiores hierárquicos, salvo em caso de legítima defesa, própria ou de outrem.

Ativos de tecnologia da informação e comunicação são todos os recursos físicos e lógicos utilizados para criar, armazenar, manusear, transportar, compartilhar e descartar a informação, independentemente se disponibilizados pela empresa ou particulares que ingressem em seu ambiente físico ou lógico. São exemplos desses recursos: microcomputador, notebook, smartphones, tablets, pendrive, mídias e impressoras.

Em razão da relevância que possuem, os ativos de tecnologia da informação e comunicação precisam estar munidos de **softwares e controles de proteção ativos e atualizados**, como antivírus, antispyware e firewall, especialmente nos **dispositivos de mobilidade**, sejam eles disponibilizados pela **TAMANDARÉ** ou particulares quando utilizados para finalidade ou em ambiente profissional.

Todo colaborador é responsável por cumprir o nível de segurança requerido pela classificação indicada na informação que tiver contato ou manusear.

Somente informações de conhecimento **PÚBLICO** podem ser divulgadas ou compartilhadas sem a necessidade de permissão prévia e expressa, por exemplo, o nome do presidente da **TAMANDARÉ ou o compartilhamento de uma propaganda que já foi disponibilizada nas mídias sociais pela empresa**. Assim, quaisquer informações classificadas como **CONFIDENCIAIS ou INTERNAS**, como o nome do cliente que contratou uma nova solução tecnológica ou o balanço da empresa, **devem ficar limitadas a determinado número de colaboradores autorizados a acessá- las em razão da atividade profissional desempenhada**.

O colaborador ou prestadores de serviço **não está autorizado a revelar, transferir, publicar, compartilhar ou divulgar quaisquer informações de propriedade ou sob a responsabilidade da empresa**, sem que haja prévia autorização para tanto, sobretudo na **internet**, nas **mídias sociais** e no âmbito acadêmico, inclusive aquelas relacionadas, mas não se limitando:

• Aos assuntos corporativos de qualquer natureza ligados à atividade exercida ou informações da empresa ou sobre ela, seus clientes, colaboradores, prestadores de serviço, fornecedores e principalmente as que possam

caracterizar quebra de confidencialidade ou sigilo. Como por exemplo, detalhes do ambiente de trabalho, a exemplo dos números de ramais, identificação dos demais colaboradores, clientes e projetos;

• Às suas rotinas de trabalho, como trajetos, horários de entrada e saída, locais de almoço, realização de reuniões e endereços de clientes. Evite comentar tarefas do seu dia-a-dia, isso pode gerar riscos à sua segurança;

•Aos dados de fornecedores, de prestadores de serviços ou de clientes, a exemplo de quais são os fornecedores ou clientes da empresa ou as soluções contratadas.

Exceto na hipótese de que a informação esteja claramente classificada como PÚBLICA.

Código Penal Art. 154 – Violação de Segredo Profissional ***Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem.***

Pena - detenção, de três meses a um ano, ou multa.

Lembre-se todos os colaboradores e prestadores de serviço são responsáveis por atender ao **sigilo profissional**, em razão de cargo ou função, **contratual e legal** em razão do **contrato ou lei específica**, além do sigilo necessário de acordo com a classificação da informação, **não podendo utilizar esse conhecimento para a obtenção de vantagens para si ou para outrem**.

O que fazer se a informação ou o documento não estiver classificado?
Recomendamos que seja aplicado o princípio da maior proteção possível, ou seja, que seja mantida a confidencialidade e que se respeite o dever de sigilo profissional.

A Identidade Digital possibilita a **geração de prova de autoria e evita o anonimato** dos atos praticados pelos colaboradores e prestadores de serviço, confirmando que foram praticados por vontade de seu único detentor.

Será que é seguro você emprestar a chave do seu carro ou da sua casa para outra pessoa?

Provavelmente não. Por isso, nunca compartilhe ou forneça sua identidade digital para terceiros! Você não quer que alguém se passe por você no ambiente digital, não é mesmo?

Código Penal: Art. 307 – Falsa identidade ***"Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:"***

Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa, se o fato não constitui elemento de crime mais grave. Seu login e sua senha, assim como o seu crachá, constituem a sua Identidade Digital e devem ser tratados de forma individual, confidencial e intransferível.

Evite a fácil identificação de sua senha. Não utilize nomes, datas especiais (ex. data de nascimento), sequencias óbvias (ex. 1234), números de telefone ou dados pessoais. Também evite anotá-la em post-its, lembretes, arquivos dentro de seu dispositivo ou qualquer outro suporte físico ou digital. **Lembre-se em manter sua confidencialidade.**

O seu crachá também identifica quem você é, sua imagem, seu nome, RG, CPF e a empresa onde trabalha constam nele. Imagine se todos que passassem ao seu lado soubessem quem você é? Por isso, quando não estiver nas dependências da **LTA-RH** guarde-o de forma segura e protegida do alcance de terceiros e não o compartilhe em hipótese alguma.

Nunca se esqueça de bloquear o recurso computacional quando se ausentar, principalmente o dispositivo mobilidade, pois, se você não tomar estes cuidados, outra pessoa poderá ter acesso direto ao seu perfil ou, até mesmo, o controle total do equipamento e das informações nele armazenadas.

Os dispositivos de mobilidade, como smartphones, aparelhos de execução de MP3, pendrives, tablets e notebooks possibilitam o acesso e compartilhamento irrestrito da informação com um número indefinido de pessoas. Contudo, trouxe novos riscos.

Todos os colaboradores e prestadores de serviço precisam observar as orientações contidas nesta **Cartilha de Segurança da Informação** no uso destas tecnologias, a fim de evitar e prevenir riscos, seja em relação ao dispositivo de propriedade da empresa ou particular em uso corporativo.

Contudo, só é permitida a conexão de dispositivos particulares na rede na corporativa quando for indispensável, relevante para o negócio da **TAMANDARÉ** e **apenas mediante autorização prévia e por escrito da Área de Tecnologia da Informação ou da Direção**.
Para garantir a confidencialidade e a integridade das informações da **TAMANDARÉ**, recomendamos que o colaborador e o prestador de serviço encerrem sempre a sessão quando não estiverem utilizando o dispositivo móvel ou serviço digital, tal qual ao término da atividade. **Evitem a exposição desnecessária de informações corporativas e bloqueiem a sua estação de trabalho e o dispositivo de mobilidade sempre após o uso**.

Não implicará em sobre jornada, sobreaviso ou plantão do colaborador a mera possibilidade de acesso remoto, porte, uso ou recebimento de informações da empresa fora do horário de expediente por meio de dispositivos móveis fornecidos pela LTA-RH ou particulares quando utilizados para finalidades profissionais, pois estes permanecem ativos ou disponíveis independentemente da vontade do colaborador ou comando da empresa.

Assim, as atividades desempenhadas fora do expediente normal dependerão de comprovação em registros adequados para serem remuneradas.

Código Penal: Art. 154-A - Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 3º - Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido.

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

Assim como ocorre nos demais ativos de tecnologia da informação e comunicação, **o antivírus, o antispyware e o**

firewall instalados nos dispositivos de mobilidade precisam permanecer sempre ativos e atualizados, a fim de dificultar a contaminação por softwares maliciosos e o vazamento de informações.

Tome muito cuidado ao utilizar redes sem fio públicas, como as encontradas em aeroportos, hotéis, restaurantes e cybercafés.

Em razão da facilidade de locomoção e da praticidade no desenvolvimento das atividades profissionais, muitas vezes deixamos as informações corporativas armazenadas nos dispositivos de mobilidade. **Contudo, hoje a informação vale dinheiro e, por isso, precisa ser adequadamente protegida!**

Desta forma, lembre-se sempre de manter a menor quantidade possível de dados corporativos e salvá-los os na rede da **TAMANDARÉ**, além de fazer backup e portar as informações da empresa com segurança (se possível mediante criptografia).

Não implicará em sobre jornada, sobreaviso ou plantão do colaborador a mera possibilidade de acesso remoto, porte, uso ou recebimento de informações da empresa fora do horário de expediente por meio de dispositivos móveis
fornecidos pela* TAMANDARÉ *ou particulares quando utilizados para finalidades profissionais, pois estes permanecem ativos ou disponíveis independentemente da vontade do colaborador ou comando da empresa.

Assim, as atividades desempenhadas fora do expediente normal dependerão de comprovação em registros adequados para serem remuneradas.

Os dispositivos de mobilidade são alvos fáceis de pessoas mal intencionadas, não só pelo valor que o equipamento representa, mas também pelas informações que estão armazenadas nele. Por isso, **mantenha uma postura discreta, utilizando dispositivos de armazenamento e transporte** (como cases, maletas, pastas e mochilas) que não chamem a atenção, porém, suficientemente resistentes e **nunca deixando tais equipamentos sozinhos** dentro de veículos, hotéis, em locais públicos ou de acesso livre.

As informações da **TAMANDARÉ** só podem estar em ambientes seguros que possibilitam a rastreabilidade, o monitoramento e garantam a confidencialidade dos dados corporativos. Neste sentido, **não é permitido utilizar**

repositórios digitais para o armazenamento ou transmissão de arquivos e informações da empresa, a exemplo, mas não se restringindo a Google Drive, SkyDrive, Dropbox, Ubuntu One, iCloud, Box, SugarSync, Skype, Google Talk, Yahoo! Messenger, Gmail, Hotmail, Yahoo! Mail, Facebook ou MSN Live. **Exceto se estiver autorizado!**

Além disso, mesmo que para agilizar o processo, **não é permitido efetuar o *upload* indevido de qualquer conteúdo ou informação de propriedade da TAMANDARÉ às plataformas de internet**, pois esses ambientes não garantem a integridade dos dados armazenados e podem permitir o acesso por pessoas não autorizadas.

O correio eletrônico corporativo possibilita o envio e o recebimento de mensagens e conteúdos em nome ou representando a **TAMANDARÉ** de maneira rápida.

Contudo, não podemos esquecer os cuidados que devemos ter quando utilizamos essa facilidade tecnológica.

Faça uso da ferramenta de caixa postal corporativa fornecida pela **TAMANDARÉ** somente para transmitir e receber informações e conteúdos profissionais ou efetuar comunicações em seu nome. Por isso, não retransmita mensagens do tipo corrente, pirâmide ou conteúdo de natureza político-partidária, brincadeiras, piadas, jogos, publicidades, propagandas, atividades comerciais, pornografia (sobretudo infantil), conteúdo pirata ou qualquer tipo de material não compatível com suas atividades, cargo, função ou infrinjam os princípios éticos e legais.

Não é permitido o uso de caixas postais particulares, serviços ou ferramentas não autorizadas previamente com finalidade corporativa, a exemplo de Hotmail, Gmail, UOL ou Terra.

***O conteúdo corporativo só pode ser acessado e transmitido através das ferramentas disponibilizadas ou autorizadas pela* TAMANDARÉ.**

Utilize esse recurso apenas para o desempenho das atividades profissionais, atendendo à lei, às políticas, normas e procedimentos da empresa, além da moral e da ética e das recomendações abaixo:

• A mesma agilidade que atendemos ao telefone e solucionamos o problema, devemos empregar nas mensagens eletrônicas corporativas. Por isso, evite que elas fiquem paradas ou sem resposta. **Consulte sua caixa de correio eletrônico ao menos duas vezes ao dia!**

• Normalmente, ao ler uma mensagem eletrônica a impressão que temos é que estamos falando com a pessoa que está do outro lado da tela.

Por isso, a linguagem precisa ser **clara e objetiva, com palavras condizentes com a finalidade e contexto profissional, isso impede o retrabalho e o entendimento dúbio;**

• **Termos que possam configurar excesso de intimidade devem ser evitados,** como por exemplo, “beijos”, “saudades”, “você é especial”. Mantenha uma postura formal e use saudações como “cordialmente”, “abraços”, “saudações” ou “atenciosamente”. **E não se esqueça** de revisar o texto antes de enviá-lo, de acordo com as normas gramaticais, **afinal que imagem você quer gerar para o seu interlocutor?**

• **Quando receber qualquer mensagem contendo alguma oferta mirabolante, conteúdos gratuitos ou prêmios inesperados, DESCONFIE!** Cuidado ao abrir mensagens e executar arquivos de origem suspeita ou desconhecida, eles podem estar infectados ou direcionar você para um site fraudulento;

• Lembre-se sempre de conferir a mensagem eletrônica antes do seu envio, **isso previne o envio de mensagens para destinatários errados.** Nunca sabemos o que a outra parte pode fazer com a mensagem que recebeu indevidamente. Contudo, se isso ocorrer, envie imediatamente outra mensagem solicitando à pessoa que desconsidere a mensagem anterior e a exclua, pois aquele conteúdo não era destinado a ela.

O recebimento de mensagens em sua caixa postal corporativa pode ocorrer em horário diverso de suas atividades profissionais estabelecidas em contrato e por si só não configuram sobre jornada nem sobreaviso. Contudo, as solicitações por este canal devem ser executadas em seu expediente normal, a menos que haja requisição expressa para que seja feito de outra forma.

A internet acarreta uma **falsa sensação de segurança e de anonimato em seus usuários**. Contudo, precisamos utilizá-la com os mesmos valores e princípios éticos que aplicamos em nossas atitudes realizadas no mundo presencial.

Dessa forma, com relação aos conteúdos acessados a partir dos recursos fornecidos pela **TAMANDARÉ** ou

particulares em uso corporativo, recomendamos que os colaboradores e prestadores de serviços **evitem** armazenar, utilizar, compartilhar ou transmitir qualquer **informação ou conteúdo que sejam:**

• Impróprios ou que atentem contra a legislação vigente, à moral, ao Código de Ética, ao Regulamento Interno, ou as políticas, normas e procedimentos da empresa.

Pense antes de agir na Sociedade Digital, pois tudo deixa rastro;

• Obscenos, eróticos, sexuais ou pornográficos, principalmente envolvendo crianças ou adolescentes, a exemplo de sites com conteúdos eróticos ou mensagens eletrônicas com fotos de pessoas nuas;

Cuidado, sua reputação e da empresa podem ser aniquiladas com apenas um clique.

Estatuto da Criança e do Adolescente (ECA) :

Art. 241-A - Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente.

Pena: reclusão, de 3 (três) a 6 (seis) anos, e multa.

• Relacionados à incitação à prática de crime, contravenção penal ou ilicitude de qualquer espécie. **Não participe de comunidades, nem publique ou envie mensagens eletrônicas com conteúdos que estimulem à prática de qualquer crime,** por exemplo: “vou jogar uma bomba no meu trabalho hoje” ou, “não suporto mais o meu chefe, alguém pode acabar com ele para mim?”;

• Agressivos, ofensivos, difamatórios, ridicularizantes, humilhantes, caluniosos, constrangedores, violentos, cruéis, abusivos ou de cunho político ou partidário. **Não faça justiça com o próprio mouse!** Por exemplo: não publique ou envie mensagens contendo sua opinião pessoal ou suas impressões sobre as características físicas, emocionais ou de apresentação pessoal sobre algum colega;

• Identificados como assédio moral ou sexual. **Constranger alguém, principalmente com o intuito de obter vantagem sexual é crime!** Por exemplo: propor um encontro que possa dar conotação de intimidade. Esteja atento ao rigor de uma critica para não humilhar o colega de trabalho perante os demais;

• Preconceituosos baseados em cor, sexo, orientação sexual, raça, nacionalidade, idade, incapacidade física ou mental, condição social, origem, religião, crença, ideologia, condição econômica ou outras situações protegidas pelas leis brasileiras.

Liberdade de expressão exige responsabilidade!

Você pode estar praticando quaisquer uns dos crimes abaixo relacionados:

Pena - detenção, de um a seis meses, ou multa Penas de reclusão que variam de um até cinco anos e multa. Pena - detenção de 6 (seis) meses a 2 (dois) anos e multa.

Pena - detenção de 1 (um) a 6 (seis) meses, ou multa.

Pena - detenção de 3 (três) meses a 1 (um) ano e multa.

Pena - detenção, de três a seis meses, ou multa.

Art. 147 do Código Penal: Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave.

Crime de Racismo – Lei º 7716 de 1989.

Art. 138 do Código Penal – Calúnia: Caluniar alguém, imputando–lhe falsamente fato definido como crime.

Art. 140 do Código Penal – Injúria: Injuriar alguém, ofendendo–lhe a dignidade ou o decoro.

Art. 139 do Código Penal – Difamação: Difamar alguém, imputando–lhe fato ofensivo a sua reputação.

Art. 286 do Código Penal: Incitar, publicamente, a prática de crime.

A **TAMANDARÉ** não permite a utilização dos ativos de tecnologia da informação e comunicação da empresa com fins de entretenimento. O colaborador não está autorizado a acessar programas de compartilhamento peer-to-peer, mídias sociais, rádios online, salas de bate-papo, jogos, blogs, fotologs ou comunicadores instantâneos, **exceto se autorizado previamente e por escrito por seu Gestor ou superior equivalente.**

Contudo, é tolerado o **acesso de forma moderada a sites de notícias, busca e institucionais**, desde que não prejudique a atenção do colaborador durante a execução das suas atividades e não comprometa a qualidade no desempenho de suas funções.

Muitas vezes, ao fotografar ou filmar algo ou alguém esquecemos que naquela imagem podem conter dados confidenciais, informações sobre a infraestrutura ou localização da empresa, e até mesmo imagem de pessoas das quais não obtemos autorização. Por isso, a **TAMANDARÉ** solicita a seus colaboradores que assinem um termo de autorização para uso de sua imagem e voz ao iniciarem suas atividades.

Contudo, às vezes, uma simples foto pode dizer muita coisa. Imagine se publicarmos uma foto nas mídias sociais, durante o dia com toda a equipe reunida em uma festa de aniversário? O que será que nossos clientes pensariam que estamos fazendo durante o expediente? E se alguma entrega estivesse atrasada em razão da alta demanda?

Por isso, **no perímetro físico da empresa não é permitido tirar fotos, filmar, captar ou reproduzir quaisquer imagens, vídeos ou sons, exceto se autorizado previamente pela TAMANDARÉ.**

É vedado, inclusive, a divulgação ou compartilhamento destes conteúdos em mídias sociais, internet ou meios eletrônicos, pois esta prática afetar a reputação e a imagem da empresa, além de ser contrária à lei.

Constituição Federal:
Art. 5º, inciso X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurando direito à indenização pelo dano material ou moral.

As mídias sociais, a exemplo do Facebook, LinkedIn, Instagram, Pinterest e Twitter, facilitam a comunicação, o compartilhamento e a troca de informações entre pessoas.

Mas, tudo que está publicado nestes ambientes se perpetua no tempo e pode ser visto fora do contexto em que foi escrito de forma globalizada e ilimitada.

Em virtude disso, recomendamos que as mídias sociais sejam utilizadas de maneira **ética, segura e legal**, independentemente se para fins corporativos ou particulares.

Liberdade de expressão exige responsabilidade e impõe limites. Escolha bem os termos, palavras, frases, textos e imagens, antes de publicá-las.

É importante lembrar que **não é permitido publicar qualquer informação ou conteúdo em nome da TAMANDARÉ ou que caracterize sua posição oficial**. Essa tarefa só é permitida por colaborador previamente autorizado e treinado para tanto. Quando você está na rua e um estranho pergunta seu nome, onde você trabalha, o que você fez hoje, qual sua balada preferida, quem são seus amigos, em que lugar foram suas ultimas férias, você responde? Provavelmente não! **Então, da mesma forma não se deve publicar essas informações para qualquer um ver e a qualquer tempo nas mídias sociais.**

Por isso, evite expor excessivamente a vida particular e rotinas, como horários, trajetos, situação financeira e de saúde, agendas, números de telefones, local de trabalho, de residência e de projetos em que está envolvido, inclusive acompanhando qualquer conteúdo associado ao seu nome, especialmente aqueles que possam comprometer a sua reputação.

Antes de publicar, compartilhar ou disseminar qualquer conteúdo verifique sua veracidade, especialmente por poder se configurar um boato ou ato vexatório a um terceiro. Muitas vezes, as comunidades e blogs que você participa falam muito sobre quem você é, por exemplo: “eu odeio meu trabalho” e “adoro sair e beber até cair”.

Proteja sua reputação digital!

Não pratique o corporate bullying, pois ele pode afetar de maneira irretratável a reputação da outra pessoa, a sua e a da empresa. Desta forma, conteúdos que desrespeitem a privacidade ou intimidade de terceiros, inclusive aqueles relacionados às características físicas, emocionais ou de apresentação, não devem ser publicados. Liberdade de expressão é diferente de abuso!

Respeite o próximo e não faça nas mídias sociais o que você não faria pessoalmente, independente se para uso particular ou profissional. Não utilize as mídias sociais para desrespeitar, humilhar ou ridicularizar outras pessoas. Evite falar mal de seus colegas, das suas atividades profissionais e fazer comentários desnecessários e negativos nas publicações ou imagens de demais usuários desses ambientes.

Esteja atento e evite interagir ou publicar conteúdo que prejudique a sua carreira profissional e sua vida particular, **pois o conteúdo divulgado nas mídias sociais pode ser lido por pessoas desconhecidas e fora do contexto imaginado.**

Os serviços na internet são pagos com as suas informações.
Dessa forma, leia sempre os termos de uso e as políticas de privacidade dos sites acessados e das mídias sociais antes de criar o seu perfil, apenas disponibilizando suas informações se concordar com as condições estabelecidas.

Recomendamos que os colaboradores responsáveis pelos canais oficiais da **TAMANDARÉ** estejam atentos ao acessar as contas de acesso das mídias sociais da empresa, principalmente quando operarem os canais corporativos e o perfil particular a partir do mesmo recurso ou dispositivo móvel. **Antes de publicar qualquer conteúdo, certifique-se que está utilizando a conta de acesso correta!**

Caso o colaborador detecte algum conteúdo publicado que afete a imagem da* TAMANDARÉ *ou de seus colaboradores, deve reportar imediatamente a ouvidoria@tamtec.com.br.

Pequenos hábitos podem fazer a diferença quando o assunto é segurança!
Você não deixaria seu carro na rua aberto ou o cofre com bens de valor destrancado.

Cuidados também devem ser aplicados na rotina corporativa:
• portáteis, tais como CDs e pendrives e dispositivos, principalmente aqueles que possuam informações internas ou confidenciais. Da mesma forma, após as reuniões, deixe o local utilizado livre de vestígios das informações ali abordadas;

• **Guarde de maneira segura e protegida os documentos e ativos de tecnologia da informação e comunicação que contenham informações internas ou confidenciais.** Quando necessário empregue as ferramentas de segurança
indicadas, **como gavetas trancadas, cofres fechados e sistemas criptográficos;**
• Esteja atento aos **documentos que você envia para a impressora.** Ao imprimir um documento, retire-o imediatamente de lá, pois, alguém não autorizado pode ter acesso a ele ou até mesmo subtraí-lo. Lembre-se de preservar os recursos corporativos. Por isso, **imprima somente o necessário;**

• Ao deixar sua estação de trabalho **realize o bloqueio de tela com senha e carregue consigo seu crachá de identificação;**

• As mídias eletrônicas que contêm informações da empresa precisam ser armazenadas em ambientes seguros e com acesso restrito, a fim de evitar que sejam acessadas por pessoas não autorizadas;

• Documentos impressos não utilizados devem ser **descartados de forma adequada.** Não é permitida a reutilização de documentos impressos com informações confidenciais.

Pratique o Descarte Seguro!

O descarte da informação é uma parte extremamente importante que compõe seu ciclo de vida. Por isso, a informação e os ativos de tecnologia da informação e comunicação devem ser descartados corretamente para impedir a recuperação, obtenção e acesso por pessoas não autorizadas.

Para garantir o descarte seguro **orientamos que os documentos, mídias e dispositivos que contenham informações confidenciais sejam completamente inutilizados e descartados por meio de incineração, destruição ou trituração.**

Cuidado com a Engenharia Social!

Ela é conhecida como uma atividade que utiliza métodos de convencimento praticados por pessoas mal intencionadas que se aproveitam da boa-fé ou ingenuidade de alguém para obtenção de informações privilegiadas, para prática de golpes e demais atos ilícitos.

Por isso, recomendamos que o colaborador tenha muito cuidado ao repassar ou transmitir informações para outras pessoas, seja de forma presencial, via telefone, Mantenha sua **mesa de trabalho limpa**, sem a exposição de papéis, mídias comunicadores instantâneos, mensagens eletrônicas ou através das mídias sociais, inclusive.

Deve-se sempre confirmar a identidade e idoneidade do solicitante ou destinatário antes do envio de informações, tal qual a real necessidade de seu compartilhamento, mesmo que solicitado por pessoa de sua confiança.

A leitura de documentos restritos ao âmbito interno da **TAMANDARÉ** em locais públicos pode facilitar o vazamento de informações, portanto não é recomendável que o colaborador carregue tais informações consigo, salvo quando estritamente necessário.

Ao conversar em locais públicos, como restaurantes, elevadores, hotéis e salas de espera, redobre o cuidado ao falar sobre assuntos relacionados à* TAMANDARÉ*, seus clientes e prestadores de serviços. Lembre-se que alguém pode prestar atenção no que você diz e utilizar essa informação indevidamente.

Toda e qualquer manutenção ou alteração de configuração dos ativos de tecnologia da informação e comunicação são responsabilidades exclusivas da Área de Tecnologia da Informação.

Em caso de perda, furto ou roubo do ativo de tecnologia da informação e comunicação da TAMANDARÉ ou particular que esteja sendo usado para finalidade ou ambiente profissional, especialmente os dispositivos de mobilidade, informe imediatamente a Área de Tecnologia da Informação, a fim de que os acessos sejam retirados e as medidas cabíveis sejam tomadas.

Além disso, não se esqueça de registrar um Boletim de Ocorrência (BO) junto à Autoridade Policial competente. ***Como medida de proteção de suas informações e de seus ativos de tecnologia da informação e comunicação, a*** **TAMANDARÉ** ***monitora todos os acessos e uso de suas informações, ativos intangíveis e ativos de tecnologia da informação e comunicação, inclusive de seus ambientes físicos e lógicos, com a captura de imagens, áudio e vídeo para proteger seu patrimônio e reputação.***

A**LTA-RH** também exerce seu direito de restringir a entrada de recursos e dispositivos tecnológicos particulares em suas instalações e efetuar auditoria e inspeções naqueles que venham interagir com suas informações ou ativos de tecnologia da informação e comunicação, a qualquer tempo e sem necessidade de aviso prévio.

Esta **Cartilha** está disponível para leitura e consulta a qualquer momento em nossa intranet (pasta O:\Politica de Segurança da Informação), juntamente com os demais documentos relacionados à segurança da informação.

Mantenha-se atualizado!

A **TAMANDARÉ** é responsável pela capacitação dos colaboradores e prestadores de serviço no uso ético, seguro e legal das suas informações e de seus ativos de tecnologia da informação e comunicação. Assim, espera-se que todos os colaboradores e prestadores de serviço cumpram com as orientações da empresa para garantir maior proteção para todos.

Os casos de **desrespeito às recomendações dessa Cartilha, bem como qualquer postura ou uso inadequado das informações e recursos computacionais da TAMANDARÉ,** ainda que por omissão ou mera tentativa de burla, justificam a aplicação de penalidades que podem envolver processo administrativo, advertência verbal ou escrita, suspensão do uso do ativo de tecnologia da informação, rescisão do contrato ou desligamento, além da

colaboração institucional com autoridades em caso de investigação, sem prejuízo da tomada de eventuais medidas judiciais cabíveis.

Respeite a legislação vigente e mantenha-se sempre atualizado sobre as recomendações de segurança da informação da empresa, praticando o uso ético, seguro e legal da tecnologia.

A **Área de Tecnologia da Informação** prestará todo o **suporte necessário ao esclarecimento de dúvidas** dos colaboradores e prestadores de serviço em relação ao uso de recursos computacionais e dos controles de proteção das informações da **TAMANDARÉ.**

Caso você tenha se envolvido ou tenha conhecimento, ainda que acidentalmente, de algum incidente, do descumprimento de qualquer disposição formal ou de uso indevido de informação ou recurso computacional da **TAMANDARÉ**, inclusive através da web, comunique imediatamente ao Responsável Segurança da Informação. O seu silêncio, em qualquer dos casos, poderá ser entendido como conluio ou má-fé, portanto, passível de punição.

Ameaça - Causa potencial de incidente indesejado, que pode resultar em danos ou perdas para um sistema ou para a empresa;

Ativo - Qualquer coisa ou recurso que tenha valor para a empresa;

Ativo Intangível - Todo elemento que possui valor para a **TAMANDARÉ** e que esteja em suporte digital ou se constitua de forma abstrata, mas registrável ou perceptível, a exemplo, mas não se limitando à reputação, imagem, marca e conhecimento;

Ativos de Tecnologia de Informação e Comunicação (ATIC) - 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:
Microcomputador, notebook, smartphones, tablets, pendrive, mídias, impressoras, scanner, entre outros. Sempre que mencionados de forma a não identificar seu possuidor ou proprietário, os ATICs compreenderão tanto os pertencentes à **TAMANDARÉ** quanto aos particulares em proveito corporativo. Caso contrário, haverá declinação de posse ou propriedade no próprio texto;

Autenticação - Etapa que valida a identificação de qualquer colaborador que deseje obter acesso a certa informação ou recurso tecnológico da **TAMANDARÉ**;

Backup – É a salvaguarda de toda a informação existente, ou parte dela, nos discos rígidos ou na rede, permitindo a recuperação de dados eventualmente perdidos ou danificados por incidente;

Colaborador - Empregado, estagiário, prestador de serviço, terceirizado, conveniado, credenciado, fornecedor, cliente, menor aprendiz, ou qualquer outro indivíduo ou Organização que venham a ter relacionamento, direta ou indiretamente, com a **TAMANDARÉ;**

Correio eletrônico corporativo - Ativo de Tecnologia da Informação e Comunicação disponibilizada pela TAMANDARÉ aos seus colaboradores para o envio e recebimento de mensagens eletrônicas internas e externas;

Dispositivos de Mobilidade - Equipamentos de pequena dimensão que têm como características a capacidade de registro, armazenamento ou processamento de informações, possibilidade de estabelecer conexões e interagir com outros sistemas ou redes, além de serem facilmente transportados devido a sua portabilidade, como por exemplo, pendrive, celular, smartphone, notebook ou netbook, tablet, equipamento reprodutor de MP3, câmeras de fotografia e/ou filmagem, ou qualquer dispositivo que permita conexão à internet (tais como dispositivos 3G) ou portabilidade ou armazenagem de dados;

Identidade Digital - É a identificação do colaborador em ambientes lógicos, sendo composta por seu login e senha ou por outros mecanismos de identificação e autenticação como crachá magnético, certificado digital, token e dados biométricos; Incidente de Segurança da Informação – É indicado por um simples ou por uma série de eventos de segurança da informação indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a si;

Informação - Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

Internet - Rede mundial de computadores, na qual o usuário pode, a partir de um computador, caso tenha acesso

e autorização, obter informação de qualquer outro computador que também esteja conectado à rede. O protocolo padrão utilizado na Internet é o TCP/IP;

Mídias Sociais - São plataformas baseadas em internet que disponibilizam a interação entre pessoas físicas ou jurídicas com a produção, troca e compartilhamento de informações de modo descentralizado;

Risco - Combinação da probabilidade de um evento e de suas consequências, que podem causar danos à empresa, perda de informações, perda financeira, parada de um serviço, entre outros;

Segurança da Informação – Preservação da confidencialidade, da integridade e da disponibilidade da informação; adicionalmente, outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas;

Violação - Qualquer atividade que desrespeite as diretrizes estabelecidas na PSI ou Normas, ou em quaisquer dos demais instrumentos regulamentares que as complementem.