ManageEngine

CARTILHA
Trabalho Remoto

Recomendações para a garantia da Segurança Jurídica e da Informação

Por Edison Fontes e Gisele Truzzi

Objetivo

Facilitar o entendimento dos gestores das organizações para implementar os controles adequados que permitam a segurança jurídica e da informação.

Recomendações apresentadas

São recomendações que os autores entendem como o padrão adequado para a Segurança Jurídica e Segurança da Informação e que permitirá uma sustentabilidade da operação de Trabalho Remoto.

As organizações podem e devem avaliar os riscos organizacionais em não implementar os controles com a rigidez apresentada neste documento. É recomendado que quando uma organização decida assumir um risco, este fato seja aprovado pelo seu Corpo Diretivo.

Evidentemente as recomendações apresentadas devem ser adaptadas ao porte, ao tipo de negócio e ao momento da organização.

As recomendações apresentadas neste documento são obrigatórias para o atendimento nível adequado de segurança jurídica e segurança da informação, conforme entendimento dos autores. Quando o texto utilizar o termo “deve”, indica obrigatoriedade no cumprimento do controle. Quando for opcional, será explicitado no texto.

Os controles de Segurança da Informação e Segurança Jurídica aqui apresentados tem como foco o Ambiente de Trabalho Remoto. Se considerarmos o Ambiente da Organização como um todo, um escopo mais abrangente, outros controles envolvendo outros aspectos precisam ser considerados. Todos os controles citados pelos autores se direcionam para a adequação do Ambiente de Trabalho Remoto.

Utilização desta Cartilha

Esta Cartilha pode ser utilizada por:

- Organizações que desejam estar em conformidade com um Padrão Básico de Segurança Jurídica e Segurança da Informação quando da utilização de Trabalho Remoto pelos seus funcionários, prestadores de serviços e similares.

- Seguradoras ou Corretoras de Seguro que oferecem o Seguro para Ambiente Cibernético, que tomaram por base os controles aqui apresentados para a aceitação dos seus clientes, em Ambiente de Trabalho Remoto.

- Associações Profissionais ou Associações Corporativas que desejam orientar seus associados quando do uso de Trabalho Remoto.

- Profissionais da Área Jurídica ou Profissionais de Segurança da Informação e Proteção de Dados Pessoais que precisam desenvolver normativos internos relacionados à Trabalho Remoto.

- Estudantes e estudiosos no assunto Proteção da Informação que desejam aprimorar seus conhecimentos em controles para a Segurança Jurídica e para a Segurança da Informação quando do uso do Trabalho Remoto.

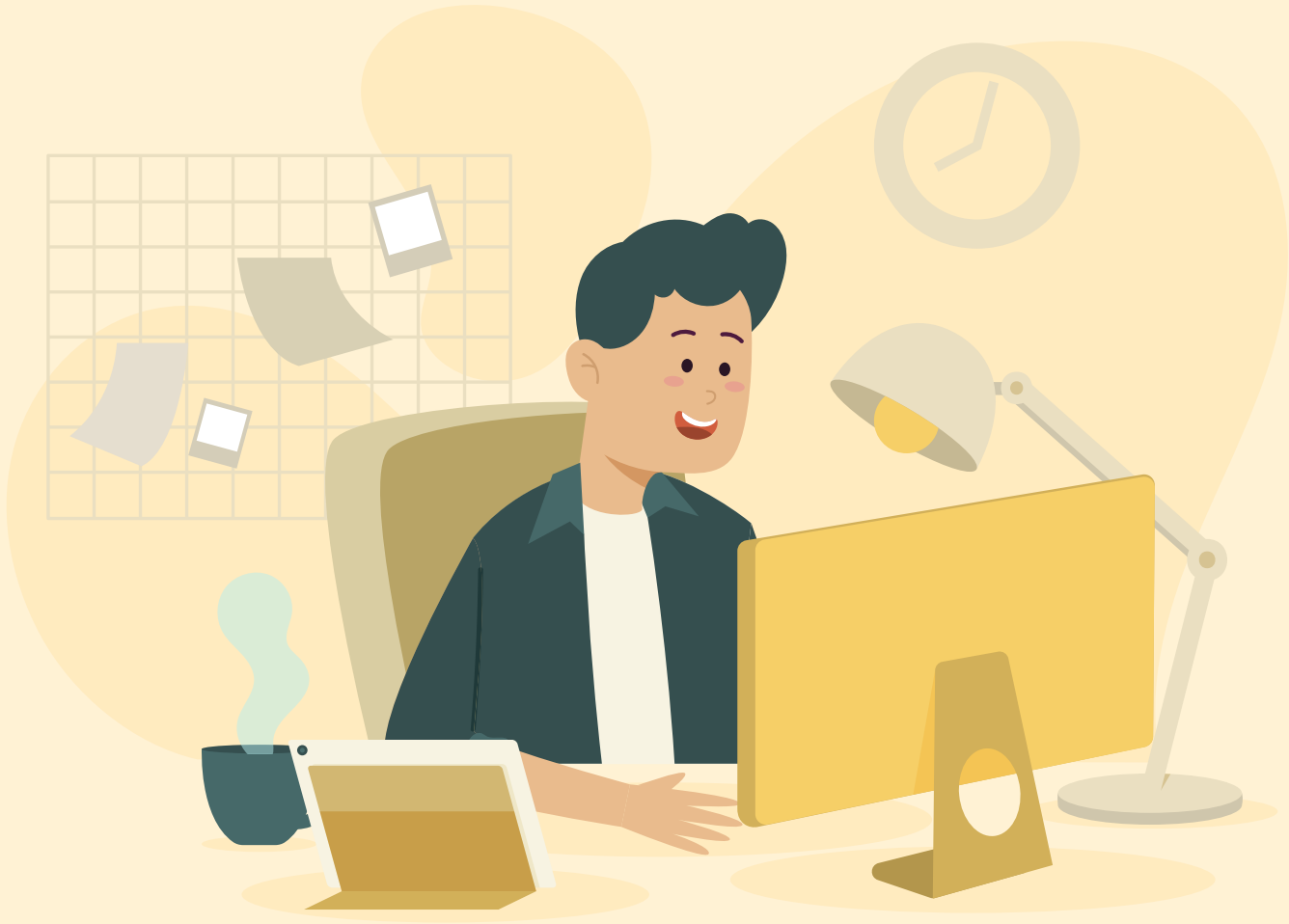
- Para você, usuário da informação e que está em Trabalho Remoto, avaliar como a sua organização considera Segurança Jurídica e Segurança da Informação nesta nova opção de você exercer suas funções profissionais.

Base Teórica e Prática

A Bibliografia apresentada no final deste documento descreve a base teórica e prática que os autores consideraram.

Evidentemente que a base prática nem sempre está documentada e é fruto da experiência dos autores em seus trabalhos realizados em diversas organizações, públicas e privadas, de diversos segmentos e de diferentes portes.

RECOMENDAÇÕES JURÍDICAS



Em situações de trabalho remoto, é essencial que a organização revise sua documentação jurídica que embasa as relações que possui com seus colaboradores, a fim de aprimorar a sua segurança, em todos os aspectos.

Pode ocorrer de ser necessária a implantação de novos documentos, tais como contratos, adendos (aditivos contratuais) ou termos, a fim de regular questões específicas sobre a nova situação de trabalho remoto.

Listamos abaixo alguns documentos jurídicos básicos e dicas importantes que você poderá levar em consideração

1. CONTRATOS DE TRABALHO – Colaboradores C.L.T.

É essencial que a organização possua contratos de trabalho assinados com seus colaboradores contratados sob regime celetista (com base na C.L.T. – Consolidação das Leis do Trabalho), também definindo questões específicas sobre o trabalho remoto. Caso o contrato já assinado anteriormente não possua uma seção específica sobre o trabalho remoto, será necessário revisar este documento, a fim de definir-se condições especiais para esta modalidade de trabalho que será desempenhada pelos colaboradores.

No contrato de trabalho, para aprimorar a segurança jurídica do trabalho remoto, é importante definir questões sobre:

- horários estimados de trabalho, tempo de disponibilidade do colaborador perante o empregador durante os dias de expediente e pontualidade: para que o empregador saiba que durante aquele período poderá contar com o colaborador, e que este deverá estar à disposição da organização;

- intervalos durante a jornada, limitações de horário do expediente, horários e dias reservados para descanso e lazer: a fim de evitar-se maiores invasões à vida pessoal e privacidade do colaborador, tendo em vista que este poderá estar trabalhando diretamente de sua residência, e que salvo raras exceções, não poderá ser importunado aos finais de semana e após o horário de trabalho, a fim de evitar-se a caracterização de horas extras;

- exclusividade: tendo em vista a habitualidade, pontualidade e subordinação do colaborador ao empregador, é necessário definir a realização do trabalho com exclusividade, a fim de proibir o colaborador de exercer a mesma atividade para outras organizações ou de forma autônoma, coibindo-se práticas relacionadas a concorrência desleal;

- uso de dispositivo móvel (notebooks, smartphones, etc.): a organização deve definir se possibilitará que o colaborador realize seu trabalho através de seus disponíveis móveis pessoais ou se fornecerá dispositivos móveis corporativos para a realização das atividades profissionais. É recomendável que, sempre que possível, a organização forneça todos os dispositivos móveis corporativos necessários ao desenvolvimento das atividades do colaborador, mediante a entrega uma Norma de Segurança da Informação (N.S.I.) de Dispositivo Móvel Corporativo, com assinatura de um Termo de Uso de Dispositivo Móvel Corporativo. Nesta N.S.I., estarão definidas todas as regras para uso dos equipamentos corporativos, permissões e vedações, deixando-se claro que o uso destes aparelhos é para fins estritamente profissionais.

- confidencialidade: é essencial a menção de uma cláusula específica ou assinatura de um termo específico sobre confidencialidade entre todos os colaboradores da organização, a fim de manterem o sigilo sobre as comunicações, assuntos tratados, trabalhos e atividades desenvolvidas, informações sobre clientes, valores, fornecedores, etc.

Caso não seja possível o fornecimento de equipamentos corporativos para desenvolvimento exclusivo das atividades profissionais, recomenda-se que a organização crie padrões específicos para a realização do trabalho remoto em dispositivos eletrônicos pessoais, definindo-se questões mínimas de segurança e comportamento exigidos para o desenvolvimento das atividades corporativas.

Tal padronização é necessária, para evitar-se que as informações da organização fiquem vulneráveis nos dispositivos pessoais dos colaboradores, ou que estes sejam negligentes quanto ao seu comportamento na internet, bem como permitindo que demais pessoais acessem o mesmo computador utilizado para suas atividades, por exemplo, colocando-se em risco a organização.

Estes padrões poderão ser implantados através de uma Norma de Segurança da Informação (N.S.I.) de Trabalho Remoto, à qual cada colaborador deverá tomar ciência; e o contrato de trabalho poderá ter uma seção específica fazendo-se referência à esta Norma.

2. CONTRATOS DE PRESTAÇÃO DE SERVIÇOS – Colaboradores PJ

Caso a organização possua colaboradores contratados como prestadores de serviço Pessoa Jurídica ("PJ"), é extremamente importante que estes contratos também sejam revisados em situações de trabalho remoto.

A contratação de um colaborador como PJ não possui tantos formalismos e detalhes quanto a contratação de um colaborador sob regime CLT, porém, não é por isso que essa relação profissional pode passar desapercebida de um contrato.

É necessário que se estabeleça no contrato de prestação de serviços, uma seção específica sobre o trabalho remoto, definindo-se padrões mínimos de segurança para desenvolvimento das atividades deste colaborador, seja em seu próprio dispositivo eletrônico, seja em dispositivo eletrônico corporativo.

Neste contrato, em cláusulas específicas, poderão ser definidas questões pontuais sobre:

- softwares e aplicativos proibidos;
- softwares e aplicativos de uso recomendados pela organização, para realização das atividades diárias;
- padrões mínimos de segurança dos dispositivos móveis (corporativos ou profissionais);
- prazos de entregas de trabalhos;
- período em que o colaborador deverá estar disponível para atendimento da organização;
- canais oficiais de comunicação com a organização;
- confidencialidade: assim como os contratos com colaboradores CLT devem conter menção específica sobre confidencialidade, é essencial que os contratos com os colaboradores PJ também possuam esse teor, a fim de manterem o sigilo sobre as comunicações, assuntos tratados, trabalhos e atividades desenvolvidas, informações sobre clientes, valores etc.

3. CONTRATO DE PRESTAÇÃO DE SERVIÇOS – Fornecedores, desenvolvedores, terceirizados e outros

A contratação de fornecedores, desenvolvedores de soluções, produtos, softwares e aplicativos, bem como de serviços terceirizados devem ser formalizadas através de um contrato de prestação de serviços específico. Em situações de emergência, caso fortuito, força maior, ou de exceção como a pandemia de covid-19 pela qual estamos passando, é possível usar as disposições deste contrato para solucionar problemas ou minimizar danos, bem como revisar determinadas condições contratadas, a fim de adequá-las à realidade enfrentada.

Nesse sentido, além das disposições comuns à esse tipo de contrato, é importante que o documento contenha também seções específicas sobre o trabalho remoto e a entrega à distância dos produtos e serviços contratados.

É importante também mencionar cláusulas específicas sobre:

- confidencialidade: resguardar o sigilo das comunicações, dos trabalhos e atividades desenvolvidas, bem como dos serviços prestados, informações acessadas, dados de clientes e demais assuntos envolvidos é essencial;

- acordo de nível de serviço (ou Service Level Agreement – S.L.A.): cláusula específica que definirá os limites de operabilidade dos serviços que envolvem tecnologia caso estes sejam interrompidos e definirá valores proporcionais para o pagamento, condizentes com o nível de disponibilidade destes serviços. (Exemplo: 100% de disponibilidade do servidor de internet em um mês = é devido 100% do pagamento contratado. 92% de disponibilidade do servidor de internet, devido a falhas ocorridas em um mês = é devido pagamento de 92% do contratado).

- política de tratamento de dados pessoais: devido à LGPD (Lei Geral de Proteção de Dados Pessoais – Lei nº 13.709/2018), é importante que a organização insira em seus contratos questões relacionadas à sua política de tratamento de dados. Tal questão poderá ser desenvolvida em um trecho específico do contrato ou poderá ser definida em uma política própria, à parte, a ser assinada entre todos os envolvidos (colaboradores CLT e PJ, prestadores de serviços e outros). É importante que a organização defina os parâmetros para o tratamento dos dados pessoais, não somente de seus clientes (eventualmente pessoas físicas), mas também de seus colaboradores, pois este tipo de informação poderá ser sensível e estará sob o manto da LGPD. Sendo assim, há necessidade de se delimitar e definir responsabilidades no tocante ao tratamento dos dados pessoais, para fins de conformidade legal e limitação de responsabilidades.

4. CONTRATOS COM CLIENTES

Os contratos firmados com os clientes podem ser padronizados, a fim de otimizar os procedimentos internos da organização, bem como podem ser bem específicos, elaborados especialmente para cada caso.

De acordo com cada nicho de negócio e questões específicas dos serviços ou produtos oferecidos aos clientes, é necessário o desenvolvimento de um contrato sólido, elaborado por advogados especializados naquela área, a fim de garantir a maior segurança jurídica possível nas relações comerciais da organização

Sendo possível o atendimento aos clientes através de trabalho remoto, é recomendável inserir tal condição no contrato, definindo-se as questões específicas vinculadas a esse assunto, tais como:

- confidencialidade e segurança da informação: não importa a forma de desenvolvimento dos serviços ou a modalidade de atendimento oferecida, é extremamente importante que a confidencialidade às informações do cliente lhe seja garantida.

Para tanto, é importante que a organização desenvolva cultura de segurança da informação, de proteção de dados e privacidade, a fim de que seus colaboradores compreendam o nível de sensibilidade e importância das informações com as quais trabalham.

É importante o uso de tecnologias seguras na comunicação interna da organização, bem como na sua comunicação com o cliente e no desenvolvimento das atividades diárias. O cliente precisa ter a sensação de que os as atividades, os serviços e produtos serão desenvolvidos com a mesma qualidade, segurança e sigilo costumeiros quando exercidos in loco. Em se falando de atividades profissionais cuja rotina de trabalho remoto não sofre qualquer interferência quando exercida nesta modalidade, é importante que o cliente tenha ciência de que a organização migrou somente de um espaço físico fixo para outros pontos, mantendo-se os mesmos padrões de excelência nos resultados entregues, o que atualmente já é possível quando utilizamos as plataformas e tecnologias adequadas.

- atendimento: é recomendável que a organização delimite horários e canais específicos de atendimento, através do trabalho remoto, para que o cliente saiba com quem e quando se comunicar.

Há diversos serviços e aplicativos gratuitos populares de mensagem, já utilizados na comunicação pessoal, que também são muito eficientes para comunicação profissional. Contudo, convém lembrar que por serem gratuitos, não há como lhes conferir 100% de segurança, e tampouco recomenda-se que informações sensíveis sejam trafegadas por ali.

Portanto, é dinâmico utilizar aplicativos, plataformas e redes sociais para comunicação com clientes, desde que a organização tenha seus pontos focais próprios para contato com o público e divulgação de suas informações com segurança (exemplo: site próprio, e-mails em domínio próprio).

- revisões de valores: em situações de resoluções de conflitos, as partes consultarão o contrato para tentar resolver os problemas. É neste sentido que uma cláusula sobre revisões de valores em situações de calamidade pública, caso fortuito ou força maior podem auxiliar a flexibilizar tais questões, dando parâmetros mínimos e máximos para eventuais renegociações.

- prazos: em situações extremas (calamidades públicas, pandemia, caso fortuito, força maior, óbitos, etc.) é necessária uma flexibilização dos prazos anteriormente definidos, pois, dependendo do caso, será praticamente impossível manter-se o mesmo prazo de entrega dos produtos ou serviços anteriormente definidos.
- flexibilização das condições negociadas: em geral, devido a situações extremas como as que já exemplificamos, faz-se necessário a revisão geral do que foi pactuado anteriormente em um contrato, devido à certas dificuldades e até mesmo impossibilidades de se manter o que foi combinado. Sendo assim, entendemos que daqui em diante, será cada vez mais necessário, termos uma seção específica nos futuros contratos, que preveja algumas flexibilizações e renegociações, em casos emergenciais.

5. ADENDOS (ADITIVOS CONTRATUAIS)

Os adendos (ou aditivos contratuais) funcionam como complementos aos contratos já firmados, atualizando-os, renovando-os ou modificando questões anteriormente já pactuadas entre as partes.

A cada nova situação consolidada entre as partes é essencial a assinatura de um novo adendo, para formalizar esta alteração ou complementação do contrato.

Em tempos de trabalho remoto ou situações emergenciais, formalizar-se as novas questões pactuadas através de adendos aos contratos é essencial, a fim de que não se gere maiores imprevistos ou insegurança jurídica.

6. TERMOS DE CONFIDENCIALIDADE (ou N.D.A. – Non Disclosure Agreement)

Questões específicas sobre sigilo e confidencialidade poderão ser discriminadas em um documento específico chamado Termo de Confidencialidade.

Nestes termos, que poderão ser assinados entre todos os colaboradores, sócios, clientes, fornecedores e prestadores de serviços da organização, podem ser definidos pontos importantes sobre a manutenção da confidencialidade das informações trafegadas, que incluem não somente os canais de comunicação da organização, bem como know-how, informações comerciais e estratégicas de negócios, planos de negócios, dados pessoais de clientes, rendimentos, bases de dados, informações sobre as atividades, produtos e serviços desenvolvidos, segredos comerciais, etc.

O Termo de Confidencialidade poderá ser assinado como um documento anexo a qualquer contrato.

Este Termo vincula as partes quanto à manutenção do sigilo e assegura a organização da não divulgação das informações sensíveis e privilegiadas pela parte assinante. Caso alguém viole as disposições deste Termo, há responsabilização nas esferas cível e criminal pela divulgação do conteúdo protegido.

7. ACORDOS DE NÍVEL DE SERVIÇO – A.N.S. (ou S.L.A. – Service Level Agreement)

Os acordos de nível de serviço podem ser firmados entre as partes em um documento próprio, no formato de um contrato específico, destinado exclusivamente a essa questão, ou podem ser transformados em uma única cláusula ou seção do contrato a ser assinado.

São cláusulas específicas que visam definir limites de operabilidade de serviços que envolvem tecnologia, caso estes sejam interrompidos, fixando-se o pagamento proporcional aos serviços entregues.

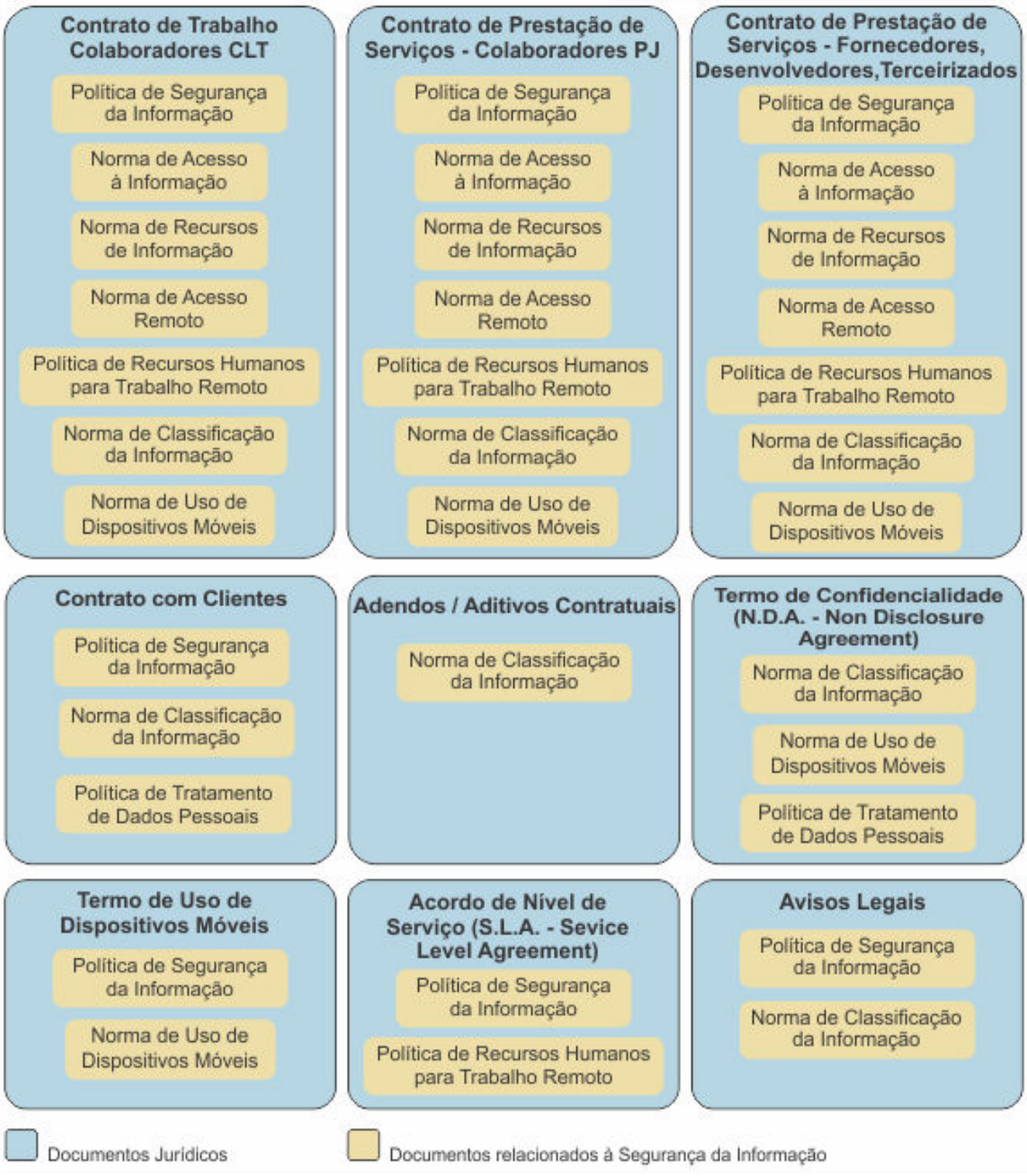
Em se tratando de situações emergenciais ou de trabalho de remoto, que envolvam a prestação de serviços de tecnologia, é recomendável que sempre tenha no contrato a previsão de um acordo de nível de serviço, a fim de que o cliente possa pagar proporcionalmente pelo serviço, de acordo com a disponibilidade deste pela organização.

8. AVISOS LEGAIS (ou Disclaimers)

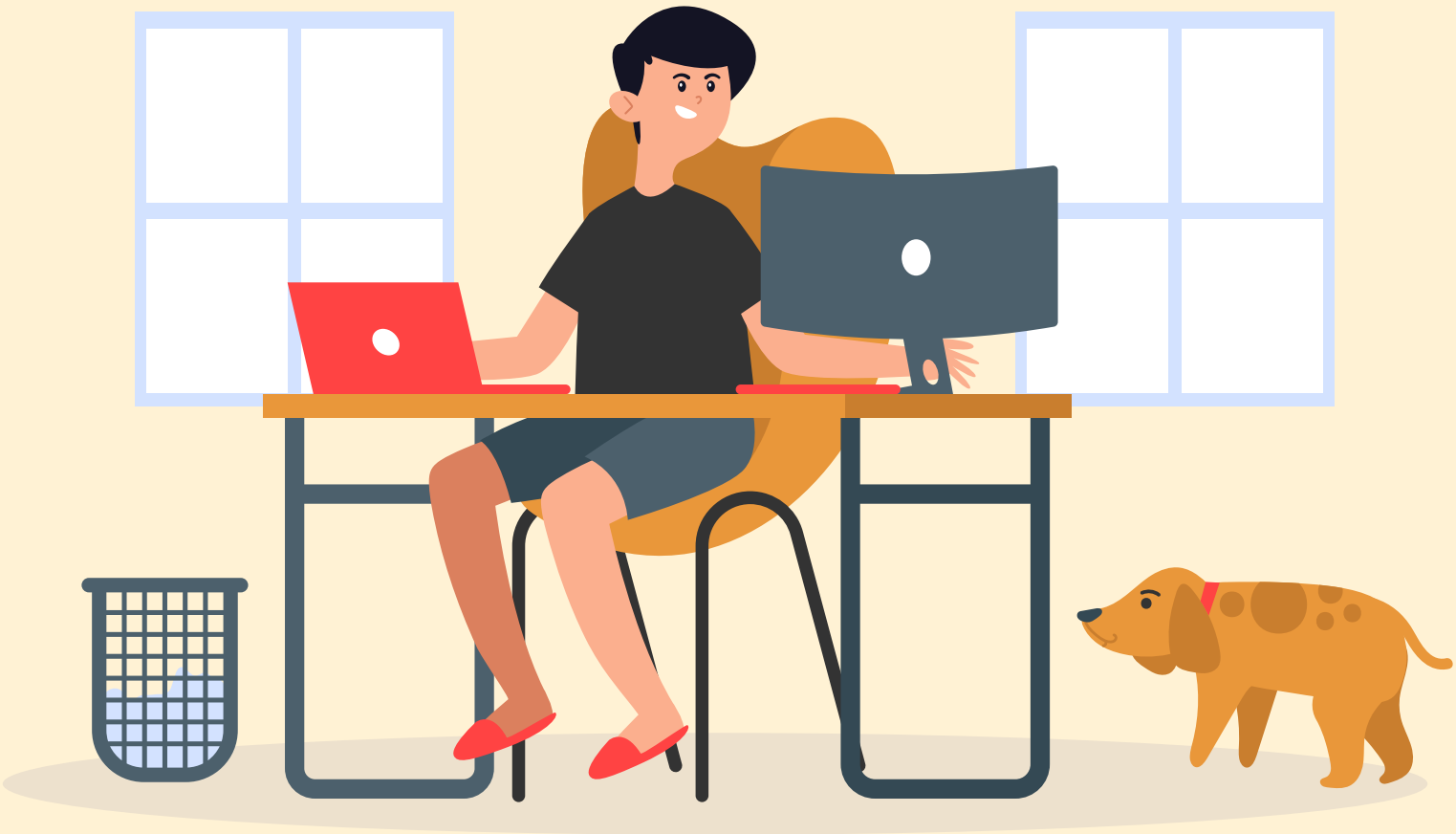
Avisos legais são pequenos textos informativos, com fundamentação jurídica, mas que visam informar ao indivíduo sobre determinada situação, de modo claro e objetivo.

São comumente vistos em rodapés de e-mails, propostas comerciais, documentos sigilos, intranet ou sistemas internos da organização, por exemplo, com a finalidade de alertar ao usuário sobre o sigilo e sensibilidade das informações acessadas.

Vínculos existentes entre alguns documentos de Segurança da Informação e documentos Jurídicos da organização, a fim de demonstrar a importância do alinhamento entre Tecnologia, Segurança da Informação e Jurídico:



CONTROLES BÁSICOS PARA SEGURANÇA DA INFORMAÇÃO



A Organização deve garantir a existência dos seguintes Controles de Segurança da Informação.

POLÍTICAS E NORMAS

1. Política de Segurança da Informação.

Regulamento que declara as diretrizes, responsabilidades e controles de como a organização se estrutura para a proteção da informação.

2. Norma de Acesso à Informação

Regulamento que define o Gestor da Informação, Gestor de Usuário, Gestor de Recursos, Gestor de Ambiente e as regras para a autorização para acesso à informação.

3. Norma Recursos de Informação

Regulamento que define regras para o uso de equipamentos de tratamento de informação, tipos de usuários que podem utilizar cada tipo de equipamento, manutenção, autorização de uso, composição dos programas e ferramentas que estarão implantados em cada tipo de equipamento. Também define uso de equipamento da organização e equipamentos particulares.

4. Norma de Acesso Remoto

Regulamento que define regras, produtos, ferramentas que devem ser utilizadas em cada tipo de equipamento, quando do acesso remoto.

5. Política de Recursos Humanos para Trabalho Remoto

Regulamento emitido pela Área de Recursos definindo todos os aspectos trabalhistas, de comportamento, de relacionamento, de registro de trabalho e outras questões relacionadas ao cuidado da pessoa e seu relacionamento profissional com a organização.

6. Norma de Gestão de Incidentes

Regulamento que define as responsabilidades e principais controles para a existência de uma efetiva Gestão de Incidentes, que deve ter um tipo de incidente relacionado ao Trabalho Remoto.

7. Norma de Uso da Internet

Regulamento que define as regras, controles e responsabilidades do usuário quando da utilização do Ambiente de Internet com recursos da organização.

8. Norma de Uso de Correio Eletrônico

Regulamento que define as regras, controles e responsabilidades do usuário quando da utilização do serviço de correio eletrônico da organização ou de correio eletrônico particular utilizando recursos da organização.

9. Norma de Uso Rede Social Pública

Regulamento que define as regras, controles e responsabilidades do usuário quando do uso de serviços de Rede Social Pública utilizando recursos da organização ou utilizando recursos particulares. Este regulamento deve explicitar como o usuário deve tratar informações sob responsabilidade da organização no Ambiente de Rede Social Pública.

10. Política de Tratamento de Dados Pessoais

Regulamento que declara as diretrizes, responsabilidades e controles de como a organização protege o tratamento de dados pessoais e explicita as responsabilidades dos usuários da organização.

11. Norma de Gestão de Riscos de Segurança da Informação

Regulamento que define as regras, controles e responsabilidades para a Gestão de Riscos de Segurança da Informação e deve contemplar o Ambiente de Trabalho Seguro.

12. Norma de Classificação da Informação

Regulamento que define as regras, controles e responsabilidades quando da classificação da informação em relação ás seguintes abordagens:

- Sigilo,
- Criticidade,
- Dado Pessoal,
- Em Atividade,
- Tipo de Coleta,
- Transparência.

13. Norma de Uso de Equipamentos – Rede Elétrica

Regulamento que define os padrões mínimos para a utilização da rede elétrica pelo equipamento em uso pelo usuário. Ambientes de Trabalho Remoto não podem utilizar soluções que podem comprometer os equipamentos utilizados.

ACESSO À INFORMAÇÃO

Cada usuário deve ter identificação individual e intransferível.

Todos os acessos e ações do usuário devem ser registradas (log).

A autenticação deve ser realizada com dois fatores de segurança. Esta exigência de dupla autenticação deve acontecer em até cada período de 4 (quatro) horas de atividade.

Quando da utilização de senhas, estas devem ser ter regras de composição com letras, números e caracteres especiais.

O usuário deve estar válido e em relacionamento profissional com a organização.

Quando do encerramento do relacionamento profissional do usuário com a organização, imediatamente ou no prazo mais curo possível, o usuário deve ter bloqueado o seu acesso ao Ambiente de informação da organização.

As autorizações de acesso do usuário aos sistemas, programas produto, pastas e demais recursos de informação devem estar autorizados pelo Gestor da Informação e devem ser validados a cada período máximo de 60 (sessenta) dias.

A organização deve definir horários de acesso por cada usuário ao Ambiente de informação da organização. Mesmo que defina como sem restrição de horário, este controle deve estar explicito e ser do conhecimento de cada usuário.

Não é permitido o uso de ferramentas, programas produto ou sistemas, no equipamento organizacional, por outra pessoa que não seja o usuário da organização.

Sistemas que são disponibilizados para os usuários como serviços e que utilizam os equipamentos apenas como um terminal de entrada/saída de informação, sem guarda de informação e sem outras facilidades, podem ser usados por usuários em equipamentos que não sejam da organização.

COMUNICAÇÃO REMOTA

A comunicação remota dos usuários utilizando qualquer recurso da organização, deve ser realizada sempre utilizando um canal seguro, tipo padrão técnico VPN.

A Área de Tecnologia e a Área de Segurança da Informação devem definir em conjunto o grau de rigidez e efetividade do canal seguro utilizado.

SERVIÇOS DE COMUNICAÇÃO INSTANTÂNEA

Comunicação interna da organização não deve utilizar Serviços de Comunicação Instantânea gratuitos. Devem ser utilizados opções corporativas, pagas e com responsabilidade contratual com o provedor de serviço.

Comunicação com clientes ao utilizar Serviços de Comunicação Instantânea devem conter apenas informações não confidencias e que se forem acessadas indevidamente, não acarretarão impactos financeiros, de reputação e operacionais. Esta comunicação não deve conter informações de conteúdo de negócio e arquivos não devem ser enviados por estas ferramentas.

USO DE EQUIPAMENTOS

Apenas equipamentos de responsabilidade da organização devem ser utilizados na comunicação e acesso ao Ambiente de informação da organização pelo usuário.

Quando do encerramento do relacionamento profissional do usuário com a organização, ou quando perda ou roubo do equipamento utilizado pelo usuário, o mesmo deve ser bloqueado o seu acesso ao Ambiente de informação da organização.

Os arquivos do equipamento organizacional utilizado pelo usuário devem estar criptografados. Somente quando do uso utilizando sistemas de controles de acesso ao equipamento e ao ambiente de informação da organização, os arquivos estarão não criptografados.

Os equipamentos devem possuir softwares de localização permitindo a organização identificar onde os mesmos estão geograficamente sendo utilizados.

Os usuários não devem ter autoridade para realizar inclusão ou exclusão de qualquer produto, ferramenta ou sistema. Qualquer inclusão ou exclusão destes recursos serão realizados remotamente pela Área de Tecnologia da Informação da organização.

Somente programas produto autorizados e padronizados pela organização podem ser executados no equipamento.

CONTINUIDADE

A organização deve ter um plano de continuidade para os casos de quebra ou roubo de equipamento organizacional utilizado pelo usuário.

Deve existir uma Central de Ajuda para o usuário consultar e resolver seus problemas em relação à questões técnicas e operacionais.

Os usuários devem estar cientes e treinados para situações de processamento em ambiente alternativo de informação da organização, quando de situações de indisponibilidade do ambiente principal de informação.

Os planos de continuidade de negócio devem ser testados até o período máximo a cada seis meses.

GESTÃO DE RISCOS DE SEGURANÇA DA INFROMAÇÃO

As ameaças para o ambiente de Trabalho Remoto devem ser consideradas na Gestão de Riscos de Segurança da Informação.

UTILIZAÇÃO DE SERVIÇOS (PLATAFORMAS, PRODUTOS OU SOLUÇÕES)

A organização deve utilizar apenas versões pagas de serviços de plataformas, produtos e soluções para tratamento de comunicação, reuniões virtuais, armazenamento, troca de informação, treinamento e similar.

Para cada serviço deve ser documentado os controles de segurança e proteção da informação utilizados na plataforma.

A utilização de serviços deve possibilitar o registro de acesso e uso, garantindo a identificação do usuário e o tratamento de informação realizado.

TREINAMENTO E COMUNICAÇÃO

Os usuários devem ser treinados periodicamente, em tempo máximo de seis meses, em segurança da informação, responsabilidades, padrões de controle de informação e proteção de dados pessoais.

A cada período de doze meses o usuário deve assinar ou revalidar o Termo de Uso da Informação.

Deve ser elaborada uma Cartilha de Trabalho Remoto – Pessoas do ambiente remoto, que devem ser entregues às pessoas que compartilham com o usuário o ambiente físico em que o usuário realiza o Trabalho Remoto.

Deve ser elaborada uma Cartilha de Trabalho Remoto – Usuário, que deve ser lida e entendida pelo usuário descrevendo como o usuário deve ser comportar, deve se apresentar, deve estar isolado e outras situações de Trabalho Remoto. Pode ser uma Cartilha ou um treinamento específico utilizando tecnologia adequada à organização, para orientar o usuário quando do Trabalho Remoto.

A Área de Recursos Humanos e a Área de Comunicação devem em conjunto enviar semanalmente um comunicado, da melhor forma adequado à organização, informando sobre a organização e mantendo o relacionamento harmonioso entre os usuários. Também deve indicar soluções e problemas do Ambiente Trabalho Remoto.

REUNIÃO REMOTA

O usuário deve garantir estar em um local com tranquilidade e sigilo adequado à reunião.

O Gestor da Reunião deve classificar a reunião em normal ou confidencial.

Para cada nível de confidencialidade de reunião (normal, confidencial) deve existir protocolos de controles de segurança para os ambientes físicos onde estarão os participantes da reunião.

Deve ser usado Fundo de Tela Virtual, padrão da organização e validado pela Área de Comunicação.

A ferramenta utilizada para Reunião Remota deve ser de licença corporativa e paga. Todos os parâmetros de segurança devem ser avaliados e ajustados pela Área de Segurança da Informação da organização.

ARMAZENAMENTO DE INFORMAÇÃO

As informações sob responsabilidade da organização devem ser sempre armazenadas no Ambiente Centralizado de Tecnologia da Informação.

Os equipamentos utilizados pelos usuários podem armazenar exclusivamente informações necessárias para a operacionalização do Trabalho Remoto. Informações utilizadas para o funcionamento e negócio da organização não podem ficar armazenadas nos equipamentos dos usuários.

SEGURANÇA FÍSICA

O ambiente físico deve ser adequadamente protegido contra a presença de pessoas não autorizadas e o seu acesso aos equipamentos.

Dependendo onde você está realizando o Trabalho Remoto, considere o uso de gravação de imagens do ambiente e do uso de cabo de segurança para o equipamento.

A ligação do equipamento à rede elétrica deve seguir padrões de utilização correta definidos em Norma de Uso de Equipamentos – Rede Elétrica.

Soluções da ManageEngine que podem auxiliar as equipes de Segurança da Informação e de TI

Log360

O Log360 é uma solução única para todos os desafios de gerenciamento de logs e segurança de rede. Ele oferece recursos de coleta, análise, monitoramento, correlação e arquivamento em tempo real que ajudam a proteger os dados confidenciais e combater ataques externos. Possui mais de 1.200 relatórios predefinidos para ajudar as empresas a atenderem às demandas mais prementes de segurança, auditoria e conformidade.

Para obter mais informações sobre o Log360,visite: *https://www.manageengine.com/br/log-management/*

AD360

Uma solução de gerenciamento de identidade e acesso (IAM) que reforça a segurança e a conformidade. Ele fornece todas essas funcionalidades para Windows Active Directory, Exchange Server e Office 365. Com essa ferramenta, você pode começar a resolver desafios de IAM no local, na nuvem e em ambientes híbridos—tudo isso a partir de um único console.

Para obter mais informações sobre o AD360, visite: *https://www.manageengine.com/br/active-directory-360/*

Desktop Central

Gerencie os endpoints de sua empresa, monitorando todos os dispositivos e sistemas em um único console e de uma dashboard exclusiva e desenvolvida para conformidade com o GDPR e a LGPD. Tenha os recursos de Gerenciamento Unificado de Endpoints (UEM) a sua disposição, como gerenciamento de patches, distribuição de software, MDM, ITAM, gerenciamento de segurança USB, segurança de navegador e muito mais.

Para obter mais informações, visite: *https://www.manageengine.com/br/desktop-central/*

DataSecurity Plus

O DataSecurity Plus é uma solução de segurança e visibilidade que oferece descobrimento de dados, análise de armazenamento de arquivos e auditoria. Ele também ajuda a atender a vários requisitos de conformidade e gera alertas instantâneos de e-mail, enquanto realiza respostas predefinidas automáticas quando potenciais ameaças de segurança ocorrem, oferecendo segurança total para todos os dados coletados e armazenados, além de controle de quem está acessando-os para evitar qualquer tipo de violação possível.

Para mais informações, visite: *https://www.manageengine.com/br/data-security/*

Password Manager Pro

O Password Manager Pro é um cofre seguro para armazenar e gerenciar informações confidenciais compartilhadas como senhas, documentos e identidades digitais de empresas. Seus recursos incluem a implantação de um cofre seguro e centralizado para armazenamento e acesso de senhas, controles de segurança preventivos através de fluxos de trabalho de aprovação e alertas em tempo real, além de auditorias da segurança para estar em conformidade regulamentar como SOX, HIPAA e PCI.

Para mais informações, visite:
https://www.manageengine.com/br/password-managerpro/

Conheça todos os produtos da ManageEngine e saiba como cada um deles pode te ajudar em outras regulamentações: www.manageengine.com/br

Sobre a ManageEngine

A ManageEngine fornece o mais amplo pacote de software de gerenciamento de TI do setor. Temos tudo que você precisa - mais de 90 produtos e ferramentas gratuitas - para gerenciar todas as suas operações de TI, desde redes e servidores a aplicações e service desk, active directory, segurança, desktops e dispositivos móveis.

Desde 2001, equipes de TI como a sua, recorreram a nós para obter um software acessível e rico em recursos, fácil de usar. Você pode encontrar nossas soluções locais e em nuvem capacitando a TI de mais de 180.000 empresas em todo o mundo, incluindo 9 em cada 10 empresas da Fortune 100. À medida que você se prepara para os desafios de gerenciamento de TI à frente, lideraremos o caminho com novas soluções, integrações contextuais e outros avanços que só podem vir de uma empresa exclusivamente dedicada a seus clientes.

E, como uma divisão da Zoho Corporation, continuaremos alinhando negócios a TI para oferecer os recursos que você precisará para aproveitar as oportunidades no futuro

AUTORES

**Gisele Truzzi é advogada especialista em Direito Digital e Segurança da Informação, proprietária de Truzzi Advogados, articulista de ISTOÉDinheiro. Atua desde 2005 na área do Direito Digital, nas esferas consultiva e contenciosa. Ministra aulas, palestras e treinamentos em todo o Brasil. É certificada em Direitos Autorais pela Harvard Law School (parceria ITS-RJ). Graduada em Direito pela Universidade Mackenzie, possui extensão em Direito Eletrônico pela FGV-RJ e pós-graduação em Gestão e Tecnologias em Segurança da Informação pela Impacta-SP. É professora convidada de cursos de pós-graduação em Direito Digital (PUC-Campinas, EPD-SP, Verbo Jurídico-SP) e autora de diversos artigos na área. É coautora da obra coletiva "Direito Digital – Debates contemporâneos" (ed. RT, 2019).*

Saiba mais em:
http://www.truzzi.com.br/quem-somos/

E-mail: contato@truzzi.com.br
www.truzzi.com.br

TRUZZI
ADVOGADOS

***Edison Fontes é Profissional de Segurança da Informação desde 1989 e possui três certificações internacionais neste assunto: CISA (Certified Information System Auditor), CISM (Certified Information Security Manager) e CRISC (Certified in Risk and Information Systems Control), todos pela ISACA/USA. É consultor da "Núcleo - Consultoria em Segurança." Possui Mestrado em Tecnologia pelo Centro Paula Souza do Governo do Estado de São Paulo, Especialização pelo Mestrado de Ciências da Computação (UFPE), Pós-Graduação em Gestão Empresarial pela FIA-USP, e Bacharelado em Informática (UFPE). É professor convidado da FIA/USP, Universidade Mackenzie, e Escola Paulista de Direito. É professor Titular da disciplina de Segurança da Informação, Especialização Privacidade e Proteção de Dados, Instituto Mauá de Tecnologia. Seu mais recente livro "Segurança da Informação: Gestão e Governança, trata das ações de proteção de dados para a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD)." Seu livro "Políticas e Normas Para a Segurança da Informação", apresenta como elaborar regulamentos e disponibiliza 30 exemplos práticos de políticas e normas, que tem sido base para muitas organizações. Possui diversos outros livros publicados sobre Segurança da Informação.*

Saiba mais em:
https://nucleoconsult.com.br/a-nucleo/equipe/

E-mail: ef@nucleoconsult.com.br
www.nucleoconsult.com.br

NÚCLEO
CONSULTORIA EM SEGURANÇA

BIBLIOGRAFIA

ABNT, NBR ISO/IEC 27001 Tecnologia da informação – Técnicas de segurança – Sistema de Gestão de segurança da informação – Requisitos. Rio de Janeiro. ABNT, 2013.

ABNT, NBR ISO/IEC 27002 - Tecnologia da informação – Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro. ABNT, 2013.

ABNT, NBR ISO/IEC 27003 – Tecnologia da Informação – Técnicas de segurança – Diretrizes para a implantação de um sistema de gestão da segurança da informação, 2011.

ABNT, NBR ISO/IEC 27004:2010 – Tecnologia da informação – Técnicas de segurança – Gestão de segurança da informação – Medição.

ABNT, NBR ISO/IEC 27005 – Tecnologia da informação – Técnicas de segurança – Gestão de riscos de segurança da informação, ABNT, 2019.

ABNT, NBR ISO/IEC 27014 – Tecnologia da informação – Técnicas de segurança – Governança de segurança da informação, ABNT, 2013.

ABNT, NBR ISO/IEC 27017 – Tecnologia da informação – Técnicas de segurança – Código de prática para controles de segurança da informação com base ABNT ISO/IEC 27002 para serviços em nuvem.

ABNT, NBR ISO/IEC 27031 – Tecnologia da informação – Técnicas de segurança – Diretrizes para a prontidão para a continuidade dos negócios da tecnologia da informação e comunicação, 2015.

ABNT, NBR ISO/IEC 27701 – Técnicas de Segurança — Extensão da ISO/IEC 27001 e ISO/IEC 27002 para Gestão da privacidade da Informação – Requisitos e diretrizes, 2019.

ABNT, NBR 31000 – Gestão de riscos – Princípios e diretrizes, ABNT, 2009.

ABNT, NBR ISO/IEC 31010 – Gestão de riscos – Técnicas para o processo de avaliação de riscos, 2012.

ABNT, NBR ISO 22301 – Segurança da Sociedade - Sistemas de gestão de continuidade de negócios – Requisitos, 2013.

ABNT, NBR ISO 22313 – Segurança da Sociedade – Sistemas de gestão de continuidade de negócios – Orientações, 2015.

FONTES, Edison. Segurança da Informação: Gestão e Governança – Para a Conformidade com a LGPD. Amazon, 2020.

Segurança da Informação – Orientações Práticas. São Paulo. Amazon, 2016.

Políticas e Normas para a Segurança da Informação, Editora Brasport, 2012.

Praticando a Segurança da Informação. Editora Brasport, 2008.

LGPD. Lei Geral de Proteção de Dados pessoais, Lei Federal No. 13.709 de 14 de agosto de 2018.

PELTIER, Thomas. Information Security Risk Analysis. USA. Auerbach, 2001.