Ketra
soluções inteligentes

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO PARA FORNECEDORES

Objetivo:

O principal objetivo do Manual de Segurança da Informação para Fornecedores é reduzir o número de possíveis riscos associados ao acesso aos Ativos de Informação e Recursos Tecnológicos da Ketra por Prestadores de Serviços, independentemente do tipo de trabalho prestado ou da relação que ligue o fornecedor à Ketra (jurídica, baseada em contrato ou qualquer outra relação não trabalhista), visando proteger a confidencialidade, integridade e disponibilidade das informações da Ketra e dos seus clientes.

A Ketra reserva-se o direito de modificar esta política quando for necessário. As alterações realizadas serão divulgadas para todas as empresas prestadoras de serviços às quais sejam aplicáveis, empregando meios considerados adequados. Cabe a cada empresa fornecedora a responsabilidade de garantir que seus colaboradores leram e tomaram conhecimento das políticas de segurança mais recentes da Ketra, assim como obter seu compromisso de obedecer e respeitar essas normas.

Caso qualquer uma dessas obrigações não seja cumprida, a Ketra reserva-se o direito de adotar, em relação à empresa contratada, medidas de penalização consideradas apropriadas, as quais poderiam chegar à dissolução de contratos em vigor com tal empresa.

Ketra
soluções inteligentes

Conceitos e definições:

- Ativos de Informação: qualquer coisa que tenha valor para a organização, como por exemplo base de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais de usuários, material de treinamento, procedimentos de suporte ou operação, planos de continuidade do negócio, procedimentos de recuperação, trilhas de auditoria e informações armazenadas. Para a Ketra, a informação é considerada um dos principais ativos.
- Ativos Físicos: equipamentos computacionais, equipamentos de comunicação, mídias removíveis e outros equipamentos;
- Backup: é uma cópia de segurança dos arquivos da empresa em dispositivos como: Storage, Núvem, HDs, CDs, DVDs e etc. Parte integrante do processo de contingência.
- Colaborador: todos os profissionais que mantenham vínculo empregatício, para toda e qualquer modalidade (Presencial, Teletrabalho, Home Office, Híbrido, Remoto) ou participação social em quaisquer das unidades da KETRA.
- Continuidade de Negócios: capacidade estratégica e tática da organização de se planejar e responder a incidentes e interrupções de negócios para conseguir continuar suas operações em um nível aceitável e previamente definido.
- Classificação da Informação: processo que compreende a identificação e definição de níveis e critérios de proteção para as informações, de forma a garantir sua confidencialidade, integridade e disponibilidade.
- Informação: Qualquer conjunto de dados que resulte em algum significado compreensível. A informação pode possuir algum valor para a Ketra, seus clientes, parceiros e colaboradores, bem como pode ser de propriedade da empresa ou estar sob sua custódia.
- Informação Restrita: quando acessos não autorizados a ela, mesmo que por membros da própria organização, sejam capazes de trazer sérios danos ao negócio.
- Informação Interna: informação que não é desejável que se torne conhecida por pessoas de fora da organização

Ketra
soluções inteligentes

Conceitos e definições:

- Informação Pública: quando a informação pode ser divulgada a todos, isto é, funcionários, terceirizados, clientes, fornecedores e público em geral, sem que isso provoque impactos no negócio.
- Informação Confidencial: quando sua exposição fora do ambiente da organização possa acarretar perdas financeiras, de imagem, de competitividade etc.
- Incidente de Segurança da Informação: interrupção não planejada ou redução na qualidade de um serviço de TI". Um simples evento ou uma série de eventos indesejados ou inesperados, que tenham uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
- Gestão de Riscos: atividades coordenadas para direcionar e controlar uma organização no que se refere a riscos de segurança da informação.
- Gestor: Colaborador que exerce cargo de liderança, como: Diretor, Gerente ou Gestor.
- Monitorar: acompanhar com objetivo de controle na gestão de TI.
- Perfis de Acesso: conjunto de acessos sistêmicos necessários para o desenvolvimento das atividades profissionais de um colaborador na organização
- Perfil Funcional: conjunto de qualificação, habilidades e responsabilidades necessárias para um colaborador desenvolver as atividades profissionais de um determinado cargo dentro da organização.
- Política de Segurança da Informação: documento que contém normas, diretrizes, procedimentos e sanções que darão subsídios para a segurança da informação.
- Prestadores de Serviços: pessoa jurídica ou física que mantenha contrato de prestação de serviço, ou tenha celebrado instrumento afim, com quaisquer prestadores de serviços prestados à Ketra.
- Proprietário da Informação: é um gestor, formalmente indicado pela diretoria, responsável por qualificar o ciclo de vida do ativo, sendo responsável também por assegurar que os ativos de informação sejam inventariados, adequadamente classificados e protegidos.
- Recurso: Qualquer ativo, tangível ou intangível, pertencente a serviço ou sob responsabilidade da Ketra, que possua valor para a empresa. Podem ser considerados recursos: pessoas, ambientes físicos, tecnologias, serviços contratados, em nuvem, sistemas e processos.

Ketra
soluções inteligentes

Conceitos e definições:

- **Recursos Tecnológicos: qualquer equipamento, sistema ou metodologia que suporte informações ou processos de negócio na organização.**
- **Segurança da Informação: É a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco, maximizar o retorno sobre os investimentos e as oportunidades do negócio.**
- **Serviços: serviços de computação e comunicações, utilidades gerais, por exemplo aquecimento, iluminação, eletricidade e refrigeração.**
- **Software: é a parte lógica do computador, ou seja, aplicativos, sistemas, ferramentas de desenvolvimento e utilitários.**
- **TIC: é a abreviação adotada para o termo Tecnologia da Informação e Comunicação. Refere-se a um conjunto de recursos tecnológicos integrados, os quais proporcionam, por meio das funções de hardware, software e telecomunicações, a automação e comunicação de processos.**
- **Usuários: termo que será utilizado para designar todas as pessoas do ambiente corporativo da Ketra, independente do cargo ocupado.**

Ketra
soluções inteligentes

Princípios Gerais de Segurança:

- Sempre que necessário, os prestadores de serviços fornecerão à Ketra uma lista de pessoas, sua descrição de perfil, funções e responsabilidades associados ao serviço prestado, comunicando todas as eventuais alterações realizadas referentes à relação com a Companhia (admissão, demissão, substituição ou alteração de funções ou cargos).
- Os prestadores de serviços deverão garantir que todos os seus colaboradores possuem a instrução adequada e estão devidamente capacitados para executar o serviço prestado, seja especificamente em relação aos campos que correspondam às atuações associadas com a prestação de serviço ou com referência à Segurança da Informação.
- Os prestadores de serviços deverão garantir, no mínimo, que todos os seus colaboradores associados ao serviço prestado tomaram conhecimento e se comprometem a obedecer ao descrito na presente política. A Ketra poderá solicitar, em qualquer momento dado, evidências do processo de divulgação destas informações.
- Os prestadores de serviços deverão permitir que a Ketra realize as auditorias de segurança que lhe sejam solicitadas, colaborando com a equipe auditora e proporcionando todas as evidências e registros requeridos.
- O alcance e a profundidade das auditorias serão expressamente definidos pela Ketra caso por caso. As auditorias serão realizadas de acordo com o planejamento estabelecido conforme o caso com o prestador de serviço.
- A Ketra reserva-se o direito de realizar auditorias extraordinárias adicionais, sempre que isto esteja devidamente justificado por causas específicas.

Ketra
soluções inteligentes

Confidencialidade das Informações:

- **Todas os Ativos de Informação, Recursos Tecnológicos, estratégias de negócio e atividades relacionadas com a Ketra ou com o seu negócio, aos quais os prestadores de serviços tenham acesso para poder desempenhar o serviço acordado, serão considerados informações confidenciais. Portanto, o acesso, troca e tratamento dessas informações deverão ser realizados de acordo com as finalidades previstas, descritas no contrato de prestação de serviços, observando o dever de manter segredo ao longo da prestação do serviço e depois que a relação com a Ketra concluir.**

- **Todos os recursos e informações aos quais possam ter tido acesso ou que tenham precisado ser elaborados, modificados ou copiados para desempenhar os serviços corretamente, serão devolvidos ao término da execução dos trabalhos. A Ketra poderá solicitar que seja realizada a exclusão segura de dados de dispositivos com os quais as informações da Ketra tenham sido acessadas.**

Ketra
soluções inteligentes

Propriedade Intelectual:

- Deverá ser garantida a observância das restrições legais relativas à utilização de material protegido pelas normas de propriedade intelectual. Os prestadores de serviços poderão utilizar apenas materiais da Ketra expressamente autorizados para o desempenho das suas funções.

- É estritamente proibido utilizar programas computadorizados em sistemas de informação da Ketra se não tiverem a licença correspondente.

- Do mesmo modo, é proibido utilizar, reproduzir, emprestar, transformar ou divulgar publicamente qualquer tipo de criação ou invenção protegida pela Lei de Propriedade Intelectual, sem a devida autorização por escrito.

- A Ketra autorizará apenas a utilização de material produzido por ela mesma ou materiais autorizados ou fornecidos pelo seu titular, de acordo com os termos e condições estabelecidos e determinados nas normas em vigor

Ketra
soluções inteligentes

Intercâmbio de Informações:

- Qualquer tipo de intercâmbio de informações produzido entre a Ketra e os prestadores de serviços, será considerado como realizado dentro do escopo estabelecido pelo respectivo contrato de prestação de serviços, de tal forma que essas informações não poderão ser empregadas fora desse escopo ou para outras finalidades.

- A distribuição de informações em formato eletrônico ou físico será realizada utilizando os recursos determinados no contrato de prestação de serviços para essa finalidade e exclusivamente para facilitação das funções associadas ao contrato em questão.

- Tendo em vista o risco detectado, a Ketra reserva-se o direito de implementar medidas de controle, registro e auditoria em relação a esses recursos de divulgação. Quanto ao intercâmbio de informações no escopo do contrato de prestação de serviços, serão consideradas não autorizadas as atuações a seguir:

✓ Transmitir ou receber material protegido por direitos autorais, violando a Lei de Proteção Intelectual.

✓ Transmitir ou receber qualquer tipo de material pornográfico, de natureza sexual explícita, declarações discriminatórias raciais ou qualquer outro tipo de declaração ou mensagem classificável como ofensiva ou ilegal.

•Transmitir ou receber informações sigilosas, exceto se a comunicação por via eletrônica estiver codificada e sua remessa autorizada por escrito.

✓ Transferir informações protegidas para terceiros não autorizados.

✓ Transmitir ou receber aplicativos não relacionados com o negócio.

✓ Participar de atividades na Internet, como grupos de notícias, jogos ou outras atividades que não estejam diretamente relacionadas com a prestação de serviços.

- Todas as atividades que possam danificar a imagem e reputação da Ketra na Internet e em qualquer outro lugar estão proibidas.

Ketra
soluções inteligentes

Utilização Inadequada de Recursos Corporativos da Ketra:

Os recursos corporativos da Ketra, aos quais os prestadores de serviços tenham acesso, deverão ser utilizados exclusivamente para cumprir com as obrigações e finalidades da prestação de serviços.

Não poderão ser usados, de forma alguma para atuações não relacionadas com a finalidade do serviço ou para realizar atividades que possam ser consideradas ilícitas, como violar a propriedade intelectual de terceiros, desobedecer à norma de proteção de dados, etc.

Os prestadores de serviços se comprometem a empregar os recursos corporativos da Ketra aos quais tenham acesso de acordo com a Política de Segurança da Informação da Ketra.

A Ketra poderá implementar mecanismos de monitoramento e auditoria que considerar adequados, tanto periodicamente ou quando resultar conveniente por questões específicas de segurança, para poder garantir a utilização adequada dos recursos mencionados.

Caso seja detectado que algum prestador de serviços ou seus colaboradores utilizam recursos ou informações da Ketra de maneira indevida, essa circunstância será comunicada ao Comitê Gestor de Segurança da Informação da Ketra, para que tome as medidas adequadas.

A Ketra reserva-se o direito de tomar as medidas cabíveis de acordo com as leis de proteção dos seus direitos.
Qualquer arquivo inserido na rede de computadores da Ketra ou qualquer equipamento conectado a ela através de meios automáticos, pela Internet, e-mail ou de qualquer outra forma, deverá cumprir com os requisitos estabelecidos na Política de Segurança da Informação da Ketra.

Ketra
soluções inteligentes

Responsabilidades do Usuário:

Os prestadores de serviços deverão garantir que todos os colaboradores que possam ter acesso aos Ativos de Informação e Recursos Tecnológicos da Ketra, no desempenho das suas funções para a Ketra, deverão respeitar os princípios definidos nos documentos:

Política de Segurança da Informação Ketra;
Política de Gestão de Incidentes de Segurança da Informação Ketra

Ketra
soluções inteligentes

Requisitos de Segurança para Dispositivos:

Todos os dispositivos que tenham acesso a informações da Ketra, independentemente de quem seja seu titular, deverão obedecer às Políticas de Segurança da Informação estabelecidas pela Ketra, observando, principalmente, as orientações do tópico “5.Política para Dispositivos Pessoais – BYOD

Ketra
soluções inteligentes

Comunicação de Incidentes de Segurança

Os prestadores de serviços se comprometem a comunicar imediatamente qualquer incidente, ponto fraco ou ameaça (observados ou suspeitados) que forem detectados nos sistemas de informação da Ketra ou que possam ter afetado informações que sejam de propriedade da Ketra ou de seus clientes, informando o Comitê Gestor de Segurança da Informação da Ketra pelo endereço de e-mail denuncia@ketra.com.br.

Em caso de colaboradores do fornecedor que trabalhem internamente na Ketra, todos os incidentes, pontos fracos ou ameaças relacionadas com as informações ou recursos da Ketra deverão ser comunicados através do endereço de e-mail denuncia@ketra.com.br

Ketra
soluções inteligentes

Princípios Específicos de Segurança:

Segurança no Desenvolvimento de Softwares:

Obrigatório para todos os prestadores de serviços que realizarem trabalhos de desenvolvimento e/ou testes de softwares para a Ketra.

- Os ambientes nos quais essas atividades sejam realizadas deverão estar isolados entre eles e dos ambientes de produção.
- Todos os processos de desenvolvimento de software terceirizado serão controlados e supervisionados pela Ketra.
- As especificações dos aplicativos deverão conter, de forma específica, os requisitos de segurança a serem observados conforme o caso.
- Os mecanismos de identificação, autenticação, controle de acesso, auditoria e integridade deverão ser incluídos em todo o ciclo de criação, desenvolvimento, implementação e operação de aplicativos.
- Os aplicativos que forem desenvolvidos deverão incluir validações dos dados de entrada que confiram que os dados estão corretos e são adequados, e que evitem a entrada de códigos executáveis
- Os processos internos desenvolvidos pelos aplicativos deverão incluir todas as validações necessárias para garantir que as informações não estão corrompidas.
- Sempre que necessário, deverão ser incluídas funções de autenticação e controle de integridade das comunicações entre os componentes dos aplicativos.
- As informações de saída, emitidas pelos aplicativos, deverão ser limitadas, garantindo que somente são disponibilizadas aquelas que forem apropriadas e necessárias.
- O acesso ao código-fonte dos aplicativos deverá estar limitado ao pessoal que presta o serviço.
- No ambiente de testes serão empregados dados reais apenas quando tiverem sido devidamente dissociados ou sempre que for possível garantir que as medidas de segurança aplicadas são equivalentes àquelas existentes no ambiente de produção.
- Durante os testes dos aplicativos, será verificado se existem vias não controladas de vazamento de informações e se as vias predefinidas recebem apenas as informações previstas.
- O ambiente de produção receberá apenas os aplicativos que tenham sido aprovados expressamente.

Ketra
soluções inteligentes

Princípios Específicos de Segurança:

Segurança dos Sistemas:

Obrigatório para todos os prestadores de serviços cujos serviços sejam prestados empregando sua infraestrutura de TIC.

Gestão de Ativos:

Os prestadores de serviços deverão contar com um registro de ativos atualizado no qual seja possível conferir os ativos empregados para a prestação do serviço.

Os prestadores de serviços deverão informar à Ketra as baixas de ativos empregados para a prestação do serviço. Se esse ativo contiver outra propriedade da Ketra (hardware, software ou outro tipo de ativo), essa deverá ser entregue à Ketra antes do procedimento de baixa, de forma que os ativos pertencentes à companhia possam ser retirados.

Sempre que um ativo contiver informações consideradas sigilosas, os prestadores de serviços deverão dar baixa nos ativos garantindo que essas informações foram eliminadas de maneira segura aplicando medidas de eliminação segura ou destruindo o ativo fisicamente de tal forma que as informações que continha não possam ser recuperadas.

Deverá haver uma pessoa responsável pelos ativos utilizados para a prestação de serviços, a qual terá que garantir que esses ativos incluem as medidas mínimas de segurança definidas pela Política de Segurança da Informação da Ketra.

O prestador de serviços garantirá que a capacidade dos sistemas é gerenciada de maneira adequada, evitando paradas em potencial ou erros de funcionamento desses sistemas devido a recursos saturados.

Erros e falhas detectados nas atividades dos sistemas deverão ser analisados, sendo adotadas as medidas necessárias para resolvê-los.

Ketra
soluções inteligentes

Princípios Específicos de Segurança:

Gerenciamento da Continuidade:

Os prestadores de serviços deverão ter um plano de continuidade e um plano de recuperação de TI para casos de desastre que permitam prestar o serviço mesmo nessas circunstâncias. Esse plano deverá ser desenvolvido com base em uma avaliação de riscos (pelo menos uma vez por ano) para fazer um levantamento de perigos que poderiam provocar a interrupção das operações e garantir que são colocadas em práticas as medidas apropriadas para seu gerenciamento e monitoramento.

Os prestadores de serviços deverão testar o plano de continuidade e o plano de recuperação, para confirmar que eles servem para restaurar o serviço dentro dos prazos estabelecidos. Esses testes deverão ser feitos uma vez por ano ou logo depois que sejam realizadas alterações, aperfeiçoamentos ou modificações importantes que afetem os serviços.

Gerenciamento de Alterações:

Os prestadores de serviços deverão garantir que todas as alterações na infraestrutura de TIC, através da qual o serviço seja prestado, estejam controladas e autorizadas, certificando-se de que nenhum componente não controlado faça parte da infraestrutura de TIC.

Será necessário verificar se todos os componentes novos incluídos na infraestrutura de TIC empregada para a prestação de serviços funcionam de maneira adequada e obedecem às finalidades para as quais foram incluídos.

Todas as alterações realizadas deverão obedecer a um procedimento estabelecido e documentado oficialmente, garantindo que as etapas de modificação correspondentes são observadas.

O procedimento de gerenciamento de alterações deverá garantir que o número de modificações referentes a componentes críticos é minimizado, ficando limitado àquelas estritamente obrigatórias.

Todas as alterações realizadas em componentes críticos deverão ser verificadas para conferir se não produzem efeitos colaterais ou imprevistos no funcionamento desses componentes ou na sua segurança.

As vulnerabilidades técnicas produzidas pelas infraestruturas empregadas para prestar os serviços deverão ser analisadas, comunicando à Ketra a todas aquelas que estejam associadas a componentes críticos, para que essas vulnerabilidades possam ser gerenciadas em conjunto.

Ketra
soluções inteligentes

OBRIGADA

Rúbia Reis

Ketra
soluções inteligentes