KPC
CONSULTORIA FINANCEIRA

POLÍTICA DE SEGURANÇA/ PROTEÇÃO/ SIGILO

Política Específica de Segurança e Proteção ao Sigilo

O tratamento das informações de uma empresa, de seus associados, de clientes e de provedores, é parte crítica na administração desta empresa.

No setor financeiro, a confidencialidade de qualquer informação que não é de domínio público tem caráter especial de grande impacto, o que exige maior cuidado.

Com o acesso e a integração de diversos meios de comunicação e informática, é necessária a formação de uma política de segurança baseada em três pilares:

1) Elaboração de Procedimentos Operacionais Relacionadas à Infraestrutura (Software e Hardware)
2) Capacitação de Pessoal (Treinamento)
3) Criação de Compromisso (Acordos de Confidencialidade)

Elaboração de Procedimentos Operacionais

Entre os procedimentos operacionais destacamos:

O uso de software e do acesso de usuários

a- A utilização do correio eletrônico (e-mail), ou qualquer outro meio de comunicação via internet (Skype, MSN, Yahoo Messenger, etc), deve ser de uso profissional. É proibida a divulgação de mensagens com conteúdo religioso, racial, pornográfico ou político. A utilização de webmail deve ser controlada por um administrador. Todo cuidado deve ser tomado ao receber arquivos suspeitos de se conter vírus;

b- Criação de filtros nos mecanismos eletrônicos de comunicação;

c- Criptografia na transmissão de arquivos de computador;

d- Proteção contra vírus existentes com o uso de softwares de prevenção que devem ser usados no servidor de rede. Periodicamente serão verificados todos os discos de armazenamento de dados (“hard-disks”) de todos os computadores;

e- Controle de acesso em que todo usuário terá uma chave de acesso à rede (login) exclusiva que identifica claramente seu detentor, acompanhada de senha de acesso controlada pela área de Informática. O supervisor da rede será o único autorizado a atribuir chaves e senhas de acesso para os usuários da rede. O perfil do usuário determinará o nível de acesso;

f- Troca periódica de senhas de acesso;

g- Segurança de arquivos: diariamente serão realizados backups de todos os arquivos de dados salvos na rede (base de dados, planilhas, textos, etc.).

Hardware – Proteção e Segurança

a- Local de instalação de hardware deve possuir proteção dos raios solares, de altas temperaturas e de incidência de poeira;

b- dimensionados para a falta de energia elétrica (para salvamento de dados e desligamento correto) e manutenção de uniformidade de tensão de rede;

c- Servidor: sala do servidor deverá possuir acesso restrito às pessoas autorizadas;

d- "Backup" externo: os arquivos de backup e a documentação dos sistemas devem ser armazenados em lugar diferente, em lugar seguro e de acesso restrito a funcionários autorizados.

e- Internet – presença de mais de um provedor em meios diferentes (wireless e cabo);

f- Uso de equipamentos de impressão aprovados pela KPC Consultoria, máquinas de fotocópia e de mecanismos eletrônicos de disseminação de informações, tais como e-mails da companhia e pessoais, internet, mensagens eletrônicas e rede de relacionamentos, etc., no sentido de que as informações sejam expostas ou reproduzidas somente em equipamentos de acesso restrito e que sejam transmitidas somente por mecanismos eletrônicos autorizados, devidamente protegidos de possíveis invasões externas, de forma a evitar a disseminação irrestrita de informações.

Capacitação Pessoal e Treinamento

O treinamento acima referido deve ser dado aos empregados da companhia que, em virtude do cargo ou da função que ocupam, tenham acesso a informações privilegiadas, neles compreendidos não apenas os que participem de processos técnicos, operacionais ou decisórios, mas também aqueles que atuem em procedimentos auxiliares.

Adoção de Comportamento Seguro

As informações sigilosas podem ser encontradas na sede da Consultoria e fazem parte do ambiente de trabalho de todos os colaboradores. Portanto, é fundamental para a proteção delas que os colaboradores adotem comportamento seguro e consistente, com destaque para os seguintes itens:

a- A atitude proativa e engajada dos colaboradores no que diz respeito à proteção das informações sigilosas;

b- Compreensão que as ameaças externas podem afetar a segurança das informações sigilosas, tais como vírus de computador, interceptação de mensagens eletrônicas, grampos telefônicos, etc., bem como fraudes destinadas a roubar senhas de acesso aos sistemas de tecnologia da informação em uso e aos servidores;

c- Assuntos relacionados ao desempenho de atividades e funções na KPC Consultoria não devem ser discutidos em ambientes públicos ou em áreas expostas como: meios de transporte, locais públicos, encontros sociais;

d- As senhas de acesso do colaborador aos sistemas da KPC Consultoria são pessoais e intransferíveis, não podendo ser compartilhadas, divulgadas a terceiros.

e- Os computadores devem ser bloqueados sempre que o colaborador se ausentar de sua estação de trabalho;

f- Arquivos eletrônicos de origem desconhecida não devem ser abertos e/ou executados nos computadores da empresa;

g- Mensagens eletrônicas e seus anexos são para uso exclusivo do remetente e destinatário e podem conter informações sigilosas;

h- O acesso remoto à rede, às informações sigilosas e sistemas da Consultoria somente será permitida mediante autorização da área de Compliance e Risco;

i- Documentos impressos e arquivos contendo informações sigilosas devem ser adequadamente armazenados e protegidos, sendo vedada a retirada da sede da consultoria sem a autorização prévia;

j- A KPC Consultoria se reserva o direito de monitorar o uso dos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus colaboradores, e que os registros e o conteúdo dos arquivos assim obtidos poderão ser utilizados para detecção de violações aos documentos internos da consultoria e, conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

Gestão de Acesso a Sistemas de Informação e a Ambientes Lógicos

Todo acesso às informações sigilosas, aos ambientes lógicos deve ser controlado, de forma a garantir acesso apenas às pessoas expressamente autorizadas pela Área de Risco e de Compliance.

O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

a- Pedido formal de concessão e cancelamento de autorização de acesso do usuário aos sistemas;

b- Utilização de identificador do Colaborador (ID de Colaborador) individualizado, de forma a assegurar a responsabilidade de cada Colaborador por suas ações e omissões;

c- Verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador e se é consistente com a Política de Segregação das Atividades;

d- Remoção imediata de autorizações dadas aos Colaboradores afastados ou desligados da Consultoria, ou que tenham mudado de função, se for o caso; e

e- Revisão periódica das autorizações concedidas.

Utilização de Internet

O uso da Internet deve restringir-se às atividades relacionadas aos negócios e serviços da KPC Consultoria, e para a obtenção de informações e dados necessários ao desempenho dos trabalhos.

Sites na Internet

O acesso à sites externos na internet é monitorado. Os arquivos contendo os registros das tentativas de acesso e dos acessos são armazenados nos servidores da consultoria.

Criação de Compromisso (Acordo de Confidencialidade)

Assinatura de acordo de confidencialidade por associados e também terceiros contratados que tenham acesso às áreas sensíveis como relacionamento com clientes, gestão de recursos e análise de risco.

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Objetivo da Segurança Cibernética

A Política de Segurança Cibernética tem como objetivo estabelecer, implementar e supervisionar um conjunto de práticas que protege a informação armazenada nos computadores, aparelhos de comunicação transmitidas através das redes de comunicações, incluindo, internet e celulares, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas.

Essa segurança também se estende a qualquer forma de comunicação de computador para computador. O código malicioso dentro de um USB seria considerado um risco de cyber espaço.

Treinamento e educação, pessoal habilitado e gestão de iniciantes podem ser incorporados pela segurança cibernética.

Conceito e Princípios

Todas as Informações sigilosas constituem ativos de valor para a Consultoria, e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a Consultoria, clientes, fundos e colaboradores.

As informações sigilosas podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos eletrônicos, mensagens eletrônicas, sites de internet, bancos de dados, meio impresso, mídias de áudio e de vídeo, dentre outras.

Cada uma dessas maneiras está sujeita a uma ou mais formas de manipulação, alteração, remoção e eliminação do seu conteúdo.

Assim, por princípio, a guarda e segurança das informações sigilosas deve abranger três aspectos básicos, destacados a seguir:

a- Acesso: Somente pessoas devidamente autorizadas pela KPC Consultoria devem ter acesso às Informações sigilosas;

b- Integridade: Somente alterações, supressões e adições autorizadas pela Consultoria devem ser realizadas às Informações sigilosas; e

c- Disponibilidade: As informações sigilosas devem estar disponíveis para os colaboradores autorizados sempre que necessário ou for demandado.

As informações sigilosas devem ser adequadamente gerenciadas e protegidas contra furto, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

A consultoria deve seguir os seguintes procedimentos para garantir a segurança cibernética:

1) Identificação e avaliação de riscos ("risk assessment");

2) Ações de prevenção e proteção;

3) Monitoramento e testes; e

4) Plano de resposta.

A responsabilidade de implantação e monitoramento desses procedimentos é da área de gestão de Risco e Compliance.

Identificação e Avaliação de Riscos ("Risk Assessment")

Os seguintes itens devem ser observados:

-Confidencialidade: garantia de que a informação é acessível somente as pessoas autorizadas.

-Integridade: salvaguarda da exatidão e completeza da informação e dos métodos de processamento.

-Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

-Riscos Cibernéticos: Riscos de ataques cibernéticos, oriundos de malware, técnicas de engenharia social, invasões, ataques de rede (DDoS e Botnets), fraudes externas, desprotegendo dados, redes e sistemas da empresa causando danos financeiros e de reputação consideráveis.

-Malwares:

-Vírus: software que causa danos a máquina, rede, softwares e banco de dados;

-Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador;

-Spyware: software malicioso para coletar e monitorar o uso de informações;

-Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.

Engenharia Social

-Pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;

-Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;

-Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;

-Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais;

-Acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

Fraudes Externas e Invasões: Realização de operações por fraudadores, utilizando-se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ações de Prevenção e Proteção

A KPC Consultoria adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância para acesso à sede e à rede, incluindo aos servidores.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados.

Ao incluir novos equipamentos e sistemas em produção, a consultoria deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

A consultoria conta com recursos anti-malware em estações e servidores de rede, como antivirus e firewalls pessoais.

A consultoria realiza, também, “backup” das informações e dos diversos ativos da instituição conforme o Plano de Contingência e de Continuidade do Negócio.

Monitoramento e Testes

A consultoria possui roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. Da mesma maneira deve diligenciar de modo a manter inventários atualizados de hardware e software atualizados, bem como os sistemas operacionais e softwares de uso atualizados.

Periodicamente, a KPC consultoria realiza testes de segurança no seu sistema de segurança da informação e proteção de dados. Seguem abaixo, algumas dessas medidas:

Ð Verificação dos logs dos colaboradores;

Ð Alteração periódica de senha de acesso dos colaboradores;

Ð Segregação de acessos;

Ð Manutenção trimestral de todo os hardwares; e

Ð “Backup” diário, realizado na nuvem.

O “backup” de todas as informações armazenadas nos servidores será realizado na forma descrita no Plano de Contingência e Continuidade de Negócios da consultoria, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

As rotinas de “backup” são periodicamente monitoradas.

Ð Plano de Resposta

Havendo indícios ou de suspeita fundamentada, a KPC Consultoria deverá ser acionada para realizar os procedimentos necessários de modo a identificar o evento ocorrido. Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento.

Na hipótese de vazamento de informações sigilosas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater ao evento identificado.

Ð Revisões e Atualizações

Esta Política será revisada ao menos uma vez por ano. Não obstante as revisões estipuladas, poderá ser alterada sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

A Área de Risco e de Compliance informará oportunamente aos colaboradores sobre a entrada em vigor de nova versão deste.