Política de Segurança da Informação

Política de Segurança da Informação

1 Introdução

1.1 Motivação

Nos tempos atuais de globalização a posse da informação significa enormes oportunidades de negócios, principalmente para uma instituição como a P&IT SOLUTION, que possui na informação o seu principal patrimônio.
Com essa motivação é que essa política de segurança da informação foi desenvolvida. Nesse documento estão explícitas um conjunto de declarações de intenções que recomenda-se para a P&IT SOLUTION.

1.2 Proposta

Esse documento descreve a Política de Segurança de bens e serviços de tecnologia da informação para a empresa P&IT SOLUTION.

1.3 Objetivos

O objetivo primário dessa política é assegurar a proteção a todas as atividades relacionadas à tecnologia da informação na empresa P&IT SOLUTION. Nela serão estabelecidos padrões de segurança da informação que visam garantir a integridade, confidencialidade e disponibilidade dos bens e serviços de tecnologia da empresa.

Outro objetivo é a necessidade de aumentar a consciência dos usuários sobre as suas responsabilidades para com a empresa P&IT SOLUTION. Alertar sobre a importância de confiabilidade e sigilo quando tratando com informações da empresa e encorajar o comportamento ético e correto a todos aqueles que utilizam os recursos computacionais da empresa.

1.4 Abrangência

Essa política é aplicada a todos os usuários, clientes, fornecedores, prestadores de serviço e visitantes que tenham ou venham a ter contato através de acesso local ou remoto a quaisquer bens e serviços de tecnologia da informação adquiridos, desenvolvidos, disponibilizados ou mantidos pela P&IT SOLUTION**.**

1.5 Revisão da Política de Segurança da Informação

1.5.1 De acordo com as necessidades de utilização de novos softwares, novos serviços ou mesmo com o surgimento de novas formas de burlar a segurança da informação da empresa, e sempre que ocorrer algo não previsto que gere dúvidas com relação a política de segurança da informação atual.

1.5.2 A revisão da Política de Segurança da Informação deve ser realizada sempre que se fizer necessário, pois como envolve diretrizes necessárias para a segurança dos usuários, dos sistemas de informação e dos serviços de tecnologias, deve manter-se sempre atualizada.

1.5.3 Sugestões de revisão por parte dos usuários também devem ser analisadas pelos responsáveis pela Política de Segurança Informação.

1.6 Divulgação desta Política

1.6.1 É obrigação da empresa divulgar a todos os seus funcionários e prestadores de serviços a política de segurança da informação. A divulgação será feita através do e-mail corporativo de cada funcionário ou prestador de serviço e será entregue uma via impressa a cada um.

1.6.2 A divulgação da política deve ser clara e ampla, para que todos os usuários tenham acesso a elas e possam compreendê-las.

1.6.3 Todo funcionário ou prestador de serviço que entrar na empresa e os já existentes devem assinar um termo de responsabilidade e de conhecimento da política de segurança da informação da empresa a fim de se evitar alegações de desconhecimento.

1.6.4 As alterações das políticas de segurança da informação devem ser comunicadas aos usuários um período antes da mesma ser implementada, para que os usuários possam adaptar-se a mesma. Fazendo com que os usuários assinem o termo de responsabilidade e de conhecimento da nova política de segurança da informação.

2 Propriedade

2.1 Os bens e serviços da tecnologia da informação utilizados pela P&IT SOLUTION são de sua propriedade e/ou custodiado de seus clientes.

2.2 Para preservar os direitos de propriedade, todos os bens e serviços de tecnologia da informação adquiridos, desenvolvidos, disponibilizados ou mantidos pela P&IT SOLUTION deverão ser protegidos através de:
Cláusulas contratuais, termos de responsabilidade e/ou outra forma legal de proteção, bem como registros de patentes quando necessário.

2.3 Não é permitido a entrada de equipamentos nem a retirada de qualquer bem da empresa, sem antes a devida autorização dada pela gerência do departamento/projeto responsável.

2.4 Como todos os bens e serviços oferecidos são de propriedade da P&IT SOLUTION, os usuários devem manter o zelo por esses bens e serviços, além de respeitar e seguir as normas propostas na Política de Segurança Informação.

2.5 Os bens e serviços são da P&IT SOLUTION, os usuários não poderão usufruir destes bens ou serviços para benefício próprio, ou de outrem senão para a empresa.

2.6 Toda informação que trafegar através da rede de computadores da P&IT SOLUTION que não estiver explicitamente identificada como propriedade de terceiros deverá ser tratada como patrimônio da P&IT SOLUTION. Esta definição tem por objetivo proibir o acesso não autorizado, 5

2.7 A divulgação, a duplicação, a modificação, a distribuição, a destruição, a perda, o uso inapropriado ou o roubo das informações de propriedade da P&IT SOLUTION

3 Políticas gerais de Segurança da Informação

A manipulação irregular, divulgação ou uso indevido da informação e dos recursos computacionais da P&IT SOLUTION é expressamente proibida. A violação dessa determinação é considerada falta grave.

Nenhum usuário pode monitorar o tráfego da rede ou simular algum dispositivo da rede, sem a devida autorização da diretoria de informática. A violação dessa determinação é considerada falta grave.

Não informar em cadastros ou listas públicas nomes completos ou e-mails pessoais ou personalizados com dados pessoais. Dê preferência aos dados do departamento ou função.

Rever periodicamente a topologia de segurança, dando prioridade à compactação do tamanho da rede existente, Sistema Operacional e Aplicativos.

Identificar qual sistema operacional fornece os melhores recursos para as aplicações requeridas.

Desabilitar as funções e comandos não necessários à boa execução dos aplicativos. Atualizar os patchs e services packs do sistema operacional e dos aplicativos.

As senhas de acesso deverão utilizar mais de 10 caracteres, dando preferência às combinações alfanuméricas e com símbolos.

Em caso de tentativas de acesso incorreto, as contas de acesso devem ser bloqueadas e um relatório de ocorrência gerado ao administrador do recurso.

Transmissão de Dados: formar um circuito de transmissão fechado e seguro (de preferência criptografado) aos dados passados. Exigir que todas as mensagens eletrônicas sejam feitas com assinatura digital validada.

O acesso remoto à rede da empresa será sempre realizado utilizando-se chamadas com CALLBACK para usuários registrados e registrar no LOG os telefones chamados pelo callback. Para esse acesso devem-se criar grupos de usuários para cada recurso disponível e montar uma topologia de grupos que oriente o administrador nas permissões que serão habilitadas.

3.1 Políticas de Log

3.1.1 É uma decisão gerencial determinar a ação a seguir com os backups de logs que se realizam. Sendo uma possibilidade de armazenar todos ou fazer uma rotação a cada backup.

3.1.2 Os dados que, preferencialmente, deverão constar nos arquivos de log de acesso a serviços disponíveis no(s) servidor(es) são os seguintes:- data- hora- endereço origem- login – serviço.
3.1.3 Para todo e qualquer serviço instalado no(s) servidor(es), deverá ser gerado um log para análise de sua utilização. 5

3.1.4 É responsabilidade do(s) Administrador(es) a análise/avaliação dos arquivos de log gerados pelos servidores da Instituição.

3.1.5 Se deve sincronizar os servidores usando qualquer protocolo como NTP, para poder analisar os logs de forma centralizada.

3.1.6 A diretoria deverá ser informada das intrusões detectadas mediante análise de logs. Assim como também deverá reportar o uso indevido dos recursos por parte dos usuários.

3.1.7 Manter os logs e registros de ocorrências por cinco anos no mínimo e armazenado em área segura e restrita.

3.2 Políticas de Backup

3.2.1 A diretoria deve determinar quais são os dados críticos da organização (ou seja, os dados que constituem a informação corporativa), incluindo cópias de segurança periódicas devem ser executadas.

3.2.2 Os usuários devem ser orientados a armazenar seus dados importantes, no servidor de arquivos da Instituição.

3.2.3 É responsabilidade do(s) Administrador(es) a execução de backups periódicos, dos dados armazenados no(s) servidor(es) de arquivos, sendo que o mesmo deve ser realizado no mínimo semanalmente, o não cumprimento deste constituí falta grave.

3.2.4 Os meios de armazenamento (fitas, CDs ou DVDs) utilizados nos backups, deverão ser armazenados em uma sala com dispositivos de segurança (contra invasão de terceiros, intempéries, incêndio, etc.), sendo que somente terão acesso a esta sala o(s) Administrador(es) da rede e a Diretoria da Instituição, ou pessoas previamente autorizadas pelos mesmos.

3.2.5 Realizar após a instalação de um servidor, uma cópia de segurança (que deve ser assinado e / ou criptografado) com informações de configuração (somente leitura) sistemas de arquivos nesse servidor.

3.2.6 A organização deve estabelecer um horário durante o qual backups e pequenas tarefas de tráfego relacionados, são realizadas para que essas tarefas não afetam a disponibilidade dos serviços.

3.3 Acesso à Internet

3.3.1 - Inclui-se nesta Política também o uso do tempo e natureza de conteúdo acessado pelos usuários, que devem sempre ser relacionados com o trabalho que o mesmo está desempenhando. Esse item é válido durante todo o tempo de permanência do usuário na empresa.

3.3.2 - Tráfego de Informações:

3.3.2.1 - Todo e qualquer arquivo ou software obtido por download originado fora da rede da P&IT SOLUTION deve ser submetido a verificação de vírus antes de ser aberto ou executado, mesmo que a origem do mesmo seja de fonte "conhecida" da P&IT SOLUTION. 4

3.3.2.2 - Toda informação obtida via Internet deve ser considerada suspeita até ser confirmada por outra fonte de informação diferente daquela que a originou.

3.3.2.3 - No caso da fonte da informação ser considerada "conhecida" da P&IT SOLUTION, e não for utilizada nenhuma ferramenta do tipo PEM (privacy enhanced e-mail) ou autenticação da origem via criptografia, a mesma deve permanecer sob suspeita.

3.3.3 - Proteção da Informação:
3.3.3.1 - Nenhuma informação considerada sigilosa pela P&IT SOLUTION pode ser enviada ou recebida via Internet sem estar devidamente protegida por métodos criptográficos de renomada eficácia.

3.3.4 Utilização dos Recursos:
3.3.4.1 - É permitido aos usuários da P&IT SOLUTION "navegar" na Internet, mas no caso dessa "navegação" ser de interesse pessoal do usuário, o mesmo deve fazê-la fora de seu horário convencional de trabalho.

3.3.5 - Controle de Acesso:
3.3.5.1 - Todo usuário da P&IT SOLUTION deve ser autenticado através do FIREWALL e utilizar um protocolo seguro para a comunicação antes de obter acesso remoto aos recursos computacionais da companhia.

3.3.6 - Correio Eletrônico:
3.3.6.1 - Propriedade: Os sistemas de correio eletrônico e todas as mensagens que através destes trafegarem, incluindo suas copias de backups são consideradas de propriedade da P&IT SOLUTION, não sendo de propriedade dos usuários do sistema.

3.3.6.2 - Uso Aceitável: Os sistemas de correio eletrônico da P&IT SOLUTION em geral devem ser utilizados apenas para negócios de interesse da companhia.

3.3.6.3 - A utilização dos sistemas de correio eletrônico da companhia para fins pessoais é permitida, contanto que:
a) Não cause sobrecarga nos recursos do sistema;
b) Não interfira na produtividade;
c) Seja executada fora de horário de trabalho ou que não seja tratada como prioridade contra as demais atividades de trabalho.

3.3.6.4 - Privilégios Gerais: Os privilégios quanto a utilização do correio eletrônico pelos usuários finais restringe-se àqueles e apenas aqueles que sejam necessários para a execução habitual de suas tarefas. Os usuários finais do correio eletrônico não devem possuir privilégios para modificar o funcionamento do sistema de correio eletrônico da companhia em qualquer aspecto. Mensagens tipo "broadcast" ou para listas internas da companhia devem ser utilizadas apenas em situações excepcionais e/ou com a permissão do administrador do sistema.

3.3.6.5 - Individualização dos Usuários: Todos os usuários do correio eletrônico da companhia devem possuir uma única conta individual no sistema, protegida por senha, e devem ser autenticados ao acessa-lo.

4 Responsabilidades

4.1 Dos usuários

4.1.1 Respeitar e cumprir as determinações da política de segurança da informação.
Todos os usuários devem respeitar as regras estabelecidas pela política de segurança da informação, sujeitos as penalidades que fazem parte do Item 5.

4.1.2 Manter a salvaguarda os recursos sob sua responsabilidade
Todos os usuários são responsáveis pela classificação das informações sob sua utilização, assim como por zelar pela manutenção de sua confidencialidade, integridade e disponibilidade.

Cada usuário deve comprometer-se com aquilo que tem acesso. Deve ainda manter segura a informação de que lhe é disponibilizada, assim como o responsável pelo sistema preocupa-se com a sua funcionalidade e segurança. Jamais o usuário em questão deve divulgar dados referentes a sua área a terceiros. Somente aquelas pessoas que devem receber a informação deste usuário é que efetivamente a terão, mesmo que tal usuário tenha "garantido" que a disseminação desta informação não comprometa os demais dados.

Senha:
A senha é a identificação daquele usuário no sistema. A senha funciona como uma assinatura digital, identificando o usuário e autorizando serviços.

4.1.3 Somente acessar os recursos sob sua responsabilidade
Se um usuário eventualmente tem acesso a uma informação que não é de sua responsabilidade, este não deve alterá-la, mesmo que o responsável por tal autorize. Em alguns casos, a boa vontade pode ser danosa, pois todos estamos sujeitos a cometer erros e alterar informações preciosas mesmo que não se tenha a intenção de fazê-lo.
Usuários são responsáveis individualmente pelos recursos alocados a eles.

4.2 – Da P&IT SOLUTION:

4.2.1 Os diretores da P&IT SOLUTION são responsáveis por garantir que a política de segurança da informação que irá ser aplicada na empresa/Instituição seja passada para todo o quadro de colaboradores.

4.2.2 Estabelecer e divulgar punições, caso o usuário venha a descumprir essa política. Essas punições devem ser claras e bem divulgadas pela empresa.

4.2.3 Definir e manter procedimentos de contingência para os recursos sob sua responsabilidade.
8

5 Penalidades

5.1 Da Falta Grave Cometida

Para efeito de Política de Segurança da Informação. Considera-se uma Falta Grave:

5.1.1 Repassar qualquer informação de exclusividade da organização P&IT SOLUTION, para terceiros ou quaisquer pessoas que não a mereçam. Facilitar meios de outras pessoas conseguirem essas informações ou mesmo ajuda-las.

5.1.2 Manipulações de quaisquer tipos de documentos eletrônicos, meios magnéticos ou mesmo o próprio desvio de informações, para um uso próprio ou de terceiros.

5.1.3 Participar de quaisquer tipos de ataques a sistemas de informação. Não importando o grau de funcionalidade do ataque.

5.1.4 Obter indevidamente acessos a recursos de qualquer natureza, que não seja de responsabilidade do indivíduo.

5.1.5 Instalações de qualquer software ou hardware que não seja de conhecimento e consentimento do setor de informática, ou mesmo que facilite acesso a informações da empresa P&IT SOLUTION.

5.2 Das disposições gerais

A empresa P&IT SOLUTION reserva-se o direito tanto no contexto administrativo como jurídico de punir as pessoas que não cumprirem de acordo a política de segurança da informação da empresa ou mesmo terem faltas graves no contexto.

Estas punições podem chegar a ser advertência, suspensão ou até mesmo a demissão do mesmo. Isso não impede que a empresa tome atitudes jurídicas baseadas na assinatura do empregado no termo de responsabilidade.

Dependendo do grau de danos à empresa, a P&IT SOLUTION reserva-se o direito de tomar as decisões que queira. Revogam-se as disposições em contrário. 9