Política de Segurança

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 XPTO, que possui na informação o seu principal patrimônio.

Com essa motivação é que essa política de segurança foi desenvolvida. Nesse documento estão explícitas um conjunto de declarações de intenções que recomenda-se para a XPTO.

1.2 Proposta

Esse documento descreve a Política de Segurança de bens e serviços de tecnologia da informação para a empresa XTPO.

A política define as diretrizes necessárias para a segurança dos bens e serviços de tecnologia da informação adquiridos, desenvolvidos, disponibilizados ou mantidos pela XPTO, visando preservar a sua integridade, confiabilidade, disponibilidade e acessibilidade.

1.3 Objetivos

O objetivo primário dessa política é assegurar a proteção a todas as atividades relacionadas à tecnologia da informação na empresa XPTO. Nela serão estabelecidos padrões de segurança 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 XPTO. 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 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 XPTO,

1.5 Revisão da Política de Segurança

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 empresa, e sempre que ocorrer algo não previsto que gere dúvidas com relação a política de segurança atual.

1.5.2 A revisão da Política de Segurança 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.

1.6 Divulgação da Política

1.6.1 É obrigação da empresa divulgar a todos os seus funcionários a política de segurança. A divulgação será feita através da publicação de uma cópia fixada no mural de cada setor.

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 que entrar na empresa e os já existentes devem assinar um termo de responsabilidade e de conhecimento da política de segurança da empresa a fim de se evitar alegações de desconhecimento.

1.6.4 As alterações das políticas de segurança 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 das novas políticas de segurança.

2 Conceitos

2.1 Funcionários
2.2 Estágiários
2.3 Coordenadores
2.4 Clientes
2.5 Visitantes
2.6 Usuários
2.7 Recursos de Hardware
2.8 Recursos de Software
2.9 Informação
2.10 Rede

3 Propriedade

3.1 Os bens e serviços da tecnologia da informação utilizados pela XPTO são de sua propriedade e/ou custodiado de seus clientes.

3.2 Para preservar os direitos de propriedade, todos os bens e serviços de tecnologia da informação adquiridos, desenvolvidos, disponibilizados ou mantidos pela XPTO deverão ser protegidos através de

cláusulas contratuais, termos de responsabilidade e/ou outra forma legal de proteção , bem como registros de patentes quando necessário.

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

3.4 Como todos os bens e serviços oferecidos são de propriedade da XPTO, os usuários devem manter o zelo por esses bens e serviços, além de respeitar e seguir as normas propostas na Política de Segurança.

3.5 Os bens e serviços são da XPTO, os usuários não poderão usufruir destes bens ou serviços para benefício próprio, ou de outrem senão para a empresa.

3.6 Toda informação que trafegar através da rede de computadores da XPTO Inc. que não estiver explicitamente identificada como propriedade de terceiros deverá ser tratada como patrimônio da XPTO Inc. Esta definição tem por objetivo proibir o acesso não autorizado, a divulgação, a duplicação, a modificação, a distribuição, a destruição, a perda, o uso inapropriado ou o roubo das informações de propriedade da XPTO Inc.

4 Políticas gerais de Segurança

A manipulação irregular, divulgação ou uso indevido da informação e dos recursos computacionais da XPTO 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 gerência 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, 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 a rede da empresa sera 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

4.1 Política de Log

4.1.1 Es una decision gerencial determinar la accion a seguir con los backups de logs que se realizan. Siendo una posibilidad almacenar todos o hacer una rotacion cada N backups.

4.1.2 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

4.1.3 Para todo e qualquer serviço instalado no(s) servidor(es), deverá ser gerado um log para análise de sua utilização.

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

4.1.5 Se deberan sincronizar los servidores usando algun protocolo como NTP, para poder analisar los logs de forma centralizada.

4.1.6 La gerencia debera ser informada de las intrusiones detectadas mediante el analisis de logs. Asi como tambien deberan reportarse el uso indebido de los recursos por parte de los usuarios.

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

4.2 POLITICAS DE BACKUP

4..2.1 En primera instancia se debe determinar cuales son los datos criticos de la organizacion (es decir los datos que constituyen la informacion corporativa) de los cuales deberan realizarse las copias de seguridad periodicas.

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

4.2.3 É responsabilidade do Administrador a execução de backup's 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.

4.2.4 Os meios de armazenamento (fitas, CD's ou DVD's) utilizados nos backup's, 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 Institúição, ou pessoas previamente autorizadas pelos mesmos.

4.2.5 Realizar despues de la instalacion de un servidor, un backup (el cual deberia estar firmado y/o encriptado) con la informacion de configuracion (read only) de los filesystems de dicho servidor.

4.2.6 Se debera establecer un horario de poco trafico durante el cual se realicen las tareas relacionadas con las copias de seguridad, de modo tal que dichas tareas no afecten la disponibilidad de los servicios.

4.3 Acesso à Internet

4.3.1 - 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 esta desempenhando. Esse item é válido durante todo o tempo de permanência do usuário na empresa.

4.3.2 - Tráfego de Informações:

4.3.2.1 - Todo e qualquer arquivo ou software obtido por download originado fora da rede da XPTO Inc. deve ser submetido a verificação de vírus antes de ser aberto ou executado, mesmo que a origem do mesmo seja de fonte "conhecida" da XPTO Inc.

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

4.3.2.3 - No caso da fonte da informação ser considerada "conhecida" da XPTO Inc., 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.

4.3.3 - Proteção da Informação:

4.3.3.1 - Nenhuma informação considerada sigilosa pela XPTO Inc. pode ser enviada ou recebida via Internet sem estar devidamente protegida por métodos criptográficos de renomada eficácia.

4.3.4 Utilização dos Recursos:

4.3.4.1 - É permitido aos usuários da XPTO Inc. "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. Bem como jogos, bate-papos e demais atividades pessoais também devem ser realizadas fora do horário de trabalho do usuário.

4.3.5 - Controle de Acesso:

4.3.5.1 - Todo usuário da XPTO Inc. deve ser autenticado através do FIREWALL e utilizar um protocolo seguro para a comunicação antes de obter acesso remoto aos recursos computacionais da companhia.

4.3.6 - Correio Eletrônico:

4.3.6.1 - Propriedade: Os sistemas de correio eletrônico e todas as mensagens que atraves destes trafegarem, incluindo suas copias back-up, são consideradas de propriedade da XPTO Inc., não sendo de propriedade dos usuários do sistema.

4.3.6.2 - Uso Aceitável: Os sistemas de correio eletrônico da XPTO Inc. em geral devem ser utilizados apenas para negócios de interesse da companhia.

4.3.6.3 - A utilização dos sistemas de correio eletrônico da compania para fins pessoais é permitida, contanto que:

a) Nao cause sobrecarga nos recursos do sistema;

b) Nao interfira na produtividade;
c) Seja executada fora de horario de trabalho ou que nao seja tratada como prioridade contra as demais atividades de trabalho.

4.3.6.4 - 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 eletronico da compania em qualquer aspecto. Mensagens tipo "broadcast" ou para listas internas da compania devem ser utilizadas apenas em situacoes excepcionais e/ou com a permissão do administrador do sistema.

4.3.6.5 - 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.

5 Responsabilidades

5.1 Dos usuários

Os funcionários são resistentes, os gerentes são resistentes, os diretores são resistentes, a presidência é resistente. Todos devem estar envolvidos no processo, as várias áreas afetadas. A metodologia utilizada será a de criar ciclos de palestras onde toda a documentação é apresentada de uma forma clara e interessante ao público. Tirar os nomes técnicos e apresentar como uma seqüência, uma estória, onde a segurança da informação é o protagonista, são adaptações das metodologias utilizadas em treinamentos de segurança do trabalho, e que funcionam.

5.1.1 Respeitar e cumprir as determinações da política de segurança

Todos os usuários devem respeitar as regras estabelecidas pela política de segurança. Deve estar claro a estes usuários que o não cumprimento das mesmas os deixarão sujeitos a punições. Antes de lhes impor estas regras é preciso, porém, um processo que venha a demonstrar-lhes o porquê destas regras. Isto evita transtornos por parte destes usuários que muitas vezes não se conformam com aquilo que lhes foi imposto.

5.1.2 Manter a salvaguarda os recursos sob sua responsabilidade

Todos os usuários (do funcionário ao presidente) são responsáveis pela classificação das informações sob sua utilização, assim como por zelar pela manutenção de sua confidencialidade, integridade e disponibilidade. Isso não é um pedido a ser feito, e sim uma premissa a ser seguida.

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. É, portanto, a prova de que aquilo que foi feito partiu deste usuário, e não de outros que se dizem ser ele. Podemos considerar a senha uma ferramenta que evita que, em muitos casos, um problema no sistema inteiro venha a ser causado por uma falha humana. Entre outras coisas, evita que usuários tenham acesso a informações não convenientes a eles e garante a informação certa a cada um dos mesmos.

A senha funciona como uma assinatura digital, identificando o usuário e autorizando serviços. O respaldo legal deste tipo de identificação é o grande responsável pela sua utilização. Como exemplos citamos fomento das transações on-line (comércio eletrônico),e pelas máquinas bancárias de auto-atendimento (cash dispenser).

5.1.3 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.

5.2 – Da XPTO:

5.3.1 Os diretores da XPTO são responsáveis por garantir que a política de segurança que irá ser aplicada na empresa/Instituição seja passada para todo o quadro de funcionários.

5.3.2 Cada departamento é responsável por garantir que os dados que estarão sob seu controle sejam guardados com sigilo, devendo garantir, caso os dados dos alunos estejam on-line, que os dados não sejam acessados e modificados.

5.3.3 Estabelecer e divulgar punições, caso o usuário venha a descumprir esse política. Essas punições devem ser clara e bem divulgadas pela empresa.

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

6 Penalidades

6.1 Da Falta Grave Cometida

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

6.1.1 Repassar qualquer informação de exclusividade da organização XPTO inc, para terceiros ou quaisquer pessoas que não a mereçam. Facilitar meios de outras pessoas conseguirem essas informações ou mesmo ajuda-las.

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

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

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

6.1.5 Instalação 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 XPTO inc.

6.2 Das disposições gerais

A empresa XPTO inc reserva-se o direito tanto no contexto administrativo como jurídico de punir as pessoas que não cumprirem de acordo a política de segurança 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 XPTO inc reserva-se o direito de tomar as decisões que queira.

Revogam-se as disposições em contrário