Faculdade Estácio de Sergipe

Pós-graduação em Segurança de Redes de Computadores

Política de Segurança da Informação da XPTO

Disciplina: Sistema de Gestão de Segurança da Informação

Prof: Adriano Lima

Grupo:

Augusto Gasparetto
Fabricio Souza
Mateus Campos
Matheus Mendonça
Paulo Rafael

Introdução

A Política de Segurança da Informação, ou PSI, é um documento no qual está determinado o universo de normas e regras que devem ser seguidas por uma organização. Tais regras precisam passar por revisões periódicas de modo a serem criticamente validadas antes de serem comunicadas aos seus funcionários. O presente documento contém uma proposta de PSI para a empresa XPTO.

Este documento orienta e estabelece as diretrizes corporativas da empresa, para elaborar uma PSI deve se levar em consideração a NBR ISO/IEC 27001, que é uma norma de códigos de práticas para a gestão de segurança da informação, onde podem ser encontradas as melhores práticas para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização.

Definição de Política de Segurança da Informação (PSI)

A política de segurança da informação (PSI) é o conjunto de ações, técnicas e boas práticas relacionadas ao uso seguro de dados. Ou seja, trata-se de um documento ou manual que determina as ações mais importantes para garantir a segurança da informação.

A PSI funciona como um código de conduta interno na empresa, ela estabelece como os funcionários devem agir, o que é proibido e o que deve ser feito em casos extremos.

Relevância de uma PSI para uma Organização

O objetivo da Política de Segurança da Informação “PSI” segundo a ISO 27002 é:

Prover orientações da Direção e apoio para a Segurança da Informação de acordo com os requisitos do negócio e com as leis e regulamentações relevantes.

A PSI define as “regras do jogo” e conduta que os colaboradores devem adotar em relação às informações da organização.

Objetivo

Estabelecer a proteção de todas as informações relacionadas ao processo de matrícula, ensino, pagamento de mensalidades, campanhas de marketing e garantir continuidade dos processos e operações.

Escopo e Abrangência

Esta política está destinada a abranger a todos aqueles que fazem parte direta e indiretamente da empresa. Deve ser aplicada e respeitada por todos sem exceção, sejam eles convidados, visitantes, alunos, professores, funcionários diretos, funcionários terceirizados, direção, presidência ou qualquer outro que venha a frequentar ou fazer uso das instalações e/ou equipamentos da XPTO.

Seu escopo engloba toda a estrutura da informação mantida e de autoria da XPTO. Além destes, os processos utilizados tanto por colaboradores quanto por alunos da instituição.

Princípios

A Segurança da Informação é tratada em um nível organizacional. Os princípios levam em conta as tomadas de decisões e considerações necessárias para que os processos da XPTO funcionem conforme desenho e implementação.

Uma abordagem voltada para riscos deve ser considerada. A segurança da XPTO deve levar em conta a proteção dos dados e comprometimento de entrega de serviços. Pontos como conformidade, competitividade no mercado, interrupções operacionais e danos a imagem da empresa devem ser considerados.

A base para segurança da informação na organização é o interesse das partes envolvidas, garantindo seus necessidades e proteção dos seus dados, assim como os dados pertencentes a XPTO. Uma prática de treinamentos e reciclagens de seus colaboradores, colabora para mitigação de riscos e para a importância do que deve ser protegido.

Diretrizes

As diretrizes para elaboração da política de segurança da informação da XPTO se inicia com a ISO 27002. Além disso é levado em conta o código de ética da empresa e os princípios da área de sistemas de informação Confidencialidade, Integridade, Disponibilidade, Autenticidade e Não repúdio.

Análise dos Processos de Negócio

A descrição dos processos está documentada em um documento dedicado, assim como a estrutura organizacionais e a arquitetura da tecnologia de informação da XPTO.

Gerenciamento da Versão e Manutenção da Política

O gerenciamento da versão deste PSI será feito com intervalos planejados e também pode ser realizado quando ocorrerem mudanças significativas na organização ou em algum processo utilizado na empresa.

Os intervalos planejados terão coincidência com o plano de re-certificação das ISO a ser executado pela empresa.

Alguma alteração significativa da XPTO também deverá acionar a revisão do PSI. Essa alteração pode ser exemplificada como mudança da estrutura organizacional. Além disso caso novos processos são instituídos (ou alteração de processos existentes), estes deverão estar de acordo com a PSI, ou atualizando a PSI a fim de garantir a excelência da segurança da informação.

Políticas de Segurança para XPTO

No desenvolvimento das políticas para a instituição de ensino XPTO, precisamos levar em conta as pessoas envolvidas. Além de funcionários temos também alunos que frequentam fisicamente a escola e acessem seu conteúdo a distância.

A política de segurança deve assegurar que todos os usuários que se relacionem com os recursos de informática.É de vital importância que todas as partes estejam cientes e envolvidos na importância da segurança da informação que a XPTO é responsável.

Para criação da política de segurança, a base foi a ISO 27002 e suas diretrizes. Além disso documentos de outras instituições de ensino foram consultadas para corroborar na criação deste documento.

Elaboração das Políticas

Política de Utilização de Rede

Este tópico visa abranger as regras de utilização da rede, incluindo login, manutenção de arquivos e tentativas de acesso não autorizadas. Os pontos são abordados discriminando usuários do sistema de rede da XPTO

Regras Gerais:

- Não é permitido a tentativa de acesso não autorizado independente dos meios utilizados;
- Não é permitido a tentativa de interferir nos serviços prestados pela XPTO;
- Ao se ausentar da estação de trabalho ou para de usar a interface EAD, o usuário deve efetuar logout da aplicação e logoff da máquina. Sendo a ausência da estação breve, deve realizar o bloqueio da máquina;

- O usuário deve fazer a manutenção do seu espaço virtual, a fim de evitar acúmulo de arquivos desnecessários e almejar a organização virtual da máquina que utiliza;

- Material de natureza pornográfica ou com intenção e potencial de instigar ações ilícitas (violência, discurso de ódio) é vedado a qualquer colaborar e usuário para ser utilizado, exposto, armazenado, distribuído, editado ou gravado, através recursos da rede ou infraestrutura da XPTO;

- Jogos ou softwares não autorizados são proibidos de serem instalados, armazenados ou distribuídos na rede da companhia. Sendo autorizado somente softwares homologados pela equipe responsável, a serem instalados por acompanhamento de responsável;

- Não é permitido criar ou remover arquivos fora a área destinada ao usuário.

A tabela abaixo descreve a área de partição de arquivos:

Diretório	Destinação
Diretório Pessoal	Arquivos pessoas de responsabilidade do usuário responsável pela partição
Diretório Departamental	Arquivos do departamento relativo a área do colaborador
Diretório da Disciplina	Arquivos da disciplina a serem utilizadas por professor e alunos
Diretório Público	Arquivos temporários ou de domínio público (Destinados a Alunos por exemplo)

- A pasta pública ou equivalente não deve ser utilizada para armazenar conteúdos de cunho sensível ou sigiloso. Este local terá uma limpeza

semestral, a fim de evitar acúmulo desnecessário de arquivos;

- Não será permitido suporte para equipamentos particulares por recursos da XPTO;

- O acesso ao ambiente de aprendizagem da XPTO, incluindo ambiente EAD, será realizado com credenciais devidamente cadastradas pela equipe técnica. O uso de contas compartilhadas fica restrito exclusivamente aos colaboradores de TI;

- A equipe de informática fica responsável por garantir a segurança da rede para proteção dos dados e do ambiente corporativo. Isso será feito através de softwares terceiros específicos contra ataques maliciosos (malware).

Regras para funcionários:

- Arquivos inerentes a empresa, devem ser armazenados na rede local, a fim de garantir a sua cópia de segurança;

- É proibido a abertura de computadores ou equipamentos de propriedade da ~~estácio.~~ Caso necessário reparo, equipe técnica deve ser acionada;

- Ao utilizar equipamentos particulares, o supervisor responsável deve ser informado;

- Ao ocorrer alteração de departamento de algum funcionário, o supervisor responsável deve garantir a atualização de acessos restritos;

- Quando ocorrer desligamento de algum funcionário, o supervisor responsável deve acionar a equipe técnica a fim de bloquear usuário. Para contas compartilhadas, as devidas alterações também serão realizadas pela equipe técnica a fim de garantir segurança das informações.

Regras para alunos:

- Ao utilizar os laboratórios de informática da instituição o aluno deve utilizar credencial destinada ao seu uso exclusivo e particular;

- Fica proibida a conexão de equipamentos externos à infraestrutura da XPTO ou aos computadores do laboratório.

Política de Administração de Contas

Este tópico visa explanar a criação, manutenção e deleção de conta, assim

como seu escopo de utilização.

Criação de contas para funcionários:

- Todo funcionário pode ter acesso a uma conta para usar recursos de informática da XPTO;
- O supervisor responsável deverá solicitar a criação da conta com indicação dos devidos acessos que ela deve possuir;
- A requisição deverá obedecer formulário disponível na rede contendo as informações descritas no documento e enviada ao e-mail designado.

Criação de contas para alunos:

- Todo aluno terá acesso a uma conta para utilizar recursos de informática da XPTO e caso seja o caso de aluno EAD, acesso ao conteúdo indicado;
- A criação da conta do aluno somente será autorizado pela supervisora de aluno da secretaria de matrícula.

Manutenção de contas:

- A equipe de informática pode bloquear qualquer conta que esteja sob suspeita de atividades impróprias ou ilícitas;
- A equipe de informática pode monitorar as contas para verificar utilização de arquivos impróprios nos diretórios pessoais.
- Contas com mais de 30 dias sem acesso serão bloqueadas pela equipe técnica.

Desativação de contas

- É reservada a ação de desativação de conta somente por parte da equipe responsável de TI da XPTO;
- Em caso de desativação de conta de funcionário, somente será permitido com autorização do supervisor responsável;
- Em caso de desativação de conta de aluno, somente será permitido com autorização do supervisor de aluno da secretária de matrícula.
- Contas com mais de 3 meses sem utilização, serão desativadas pela equipe técnica.

Política de Senhas

- Senhas serão utilizadas para validação de identidade no acesso aos computadores das dependências da XPTO, assim como acesso ao conteúdo EAD da empresa;

- Na criação de novas contas, senhas temporárias são fornecidas com validade de 72 horas. Ao serem utilizadas, o sistema automaticamente solicitará a criação de nova senha definitiva;

- A política de alteração de senha é solicitada pelo sistema a cada 3 meses;

- Na tentativa de utilização de uma senha incorreta por 5 vezes, a conta é bloqueada. Para solicitar desbloqueio o funcionário deve solicitar o departamento responsável e o aluno deve solicitar ajuda na secretaria;

- As senhas são sigilosas e intransferíveis e cabe aos usuários o seu devido cuidado;

- A senha deverá ter no mínimo 8 dígitos com pelo menos: 1 letra maiúscula, 1 letra minúscula, 1 numeral e 1 caractere especial.

Política de Utilização dos E-mails

- Os e-mails devem ser utilizados de forma consciente, evitando linguajar e conteúdo impróprio para o ambiente corporativo, sendo exclusivos de funcionários da XPTO;

- O e-mail corporativo não deve ser utilizado para fins pessoais, como cadastro em sites externos ou recebimento de mala direta;

- A equipe técnica poderá bloquear o e-mail que estiver sendo utilizado a perturbar o ambiente de trabalho;

- A cota máxima por pessoa é de 300 Mb para armazenamento dos e-mails. Fica sob sua responsabilidade a manutenção da mensagens a serem armazenadas;

- É obrigatório uso do software Outlook, o qual foi homologado, para utilização de cliente de e-mail;

- É vedado a abertura de e-mail de remetentes desconhecidos suspeitos;

- É vedado a abertura de anexos de qualquer remetente desconhecido;

- É obrigatório uso de assinatura padrão da XPTO.

Política de Acesso a Internet

- O acesso a internet deve ser utilizado com fins de trabalho ou estudo, sendo vedado seu uso recreativo no horário de trabalho ou de aula;

- É proibido a divulgação de informações confidenciais da XPTO em sites da internet, grupos de discussões, chats de bate-papo;

- Caso seja necessário, a equipe de informática da XPTO poderá bloquear páginas e acessos que comprometam a segurança da instituição, uso de banda e bom andamento de trabalhos;

- É obrigatório o uso dos navegadores Mozilla ou Internet, que foram homologados pela equipe responsável da XPTO.

Política de Descartes

- O descarte de equipamentos antigos pode ser feitos somente pela equipe de informática;

- Os disco-rígidos a serem descartados, devem antes serem incapacitados de serem utilizados, a fim de evitar roubo ou apropriação de informação confidencial;

- Softwares que não são mais utilizados devem ter uma cópia da mídia de instalação armazenada caso seja necessário acessar suas informações ou conteúdo;

- Bases de dados que não mais serão utilizadas, devem permanecer armazenadas em arquivo caso precisem ser consultadas, não necessitando de sua disponibilidade imediata;

Organização da Segurança da Informação

Organização Interna

Esta seção explora a as partes envolvidas internamente a organização que se relacionam diretamente com a segurança da informação.

Comprometimento da Direção

O apoio por parte da direção se dá com a elaboração desta documentação. Além disso com a aprovação da política desenvolvida para a segurança da informação da XPTO.

Coordenação da Segurança da Informação

A coordenação da política ficará sob responsabilidade da comissão formada para elaboração e implementação do PSI. São eles o Diretor geral, funcionários de

TI, responsável pela assessoria jurídica, coordenador administrativo-financeiro e coordenador pedagógico.

Atribuição de Responsabilidades

A coordenação de segurança da informação será consultada e fará a nomeação e atribuição de responsabilidades para tarefas específicas a serem executadas ao longo do desenvolvimento da PSI.

Processo de Autorização de Novos Recursos

Para utilização de novos recursos, como software e hardware, deverão estes passar por validação e homologação da equipe responsável de informática.

Acordo de Confidencialidade

Acordo de confidencialidades são assinados por todas as partes envolvidas com as informações de propriedade da XPTO.

Para funcionário é assinado acordo assim que a contratação se torna efetiva, responsabilidade do RH.

Para alunos, no ato da matrícula é assinado um termo de confidencialidade ser cumprido pelo aluno. Este acordo expressa a ciência do cliente em não divulgar e comercializar aulas e conteúdo de propriedade da XPTO.

Parceiros e funcionários terceiros contratados também terão acordos de confidencialidade a serem assinados com responsabilidade da área de contratação e do setor jurídico.

Gestão de Ativos

A NBR ISO 27002 define como objetivo principal para a gestão de ativos alcançar e manter a proteção adequada dos ativos da organização. Para atingir essa meta, a XPTO possui as algumas características em sua gestão de arquivos, que serão listadas a seguir.

Vale lembrar que uma gestão de ativos bem feita começa no planejamento e decisão de aquisição de um bem. A gestão precisa fazer com que a XPTO como um todo tire um melhor proveito de todos os seus ativos. Caso a referida gestão seja ineficaz, os ativos podem vir a ser subutilizados ou mal dimensionados. A partir do momento em que a empresa não extrai o máximo de seus ativos, ela consequentemente deixa de agregar valor através dos mesmos.

É preciso conhecer os ativos a serem geridos, por isso deve existir na XPTO um inventário de todos os seus ativos para um correto e eficaz controle dos mesmos. Tal inventário deve conter o registro de cada ativo bem como algumas de suas qualidades e características.

Todo colaborador que possua o porte de determinado ativo, será considerado seu proprietário. Todo proprietário é responsável pela manutenção e devida utilização dos ativos sob sua responsabilidade. Todas as regras estipuladas nesta PSI referentes ao uso dos ativos devem ser respeitados pelos seus utilizadores.

Do ponto de vista da gestão da informação como ativo, deve ser classificada em níveis diferentes de proteção de acordo com sua prioridade e necessidade pré-estabelecidas para a XPTO. O estabelecimento dessas prioridades é diretamente proporcional ao valor da informação para a organização, bem como seu requisito legal, criticidade e sensibilidade. Os dados cadastrais dos alunos da XPTO bem como as informações financeiras da empresa, por exemplo, devem ser considerados de altíssimo grau para proteção e garantia de integridade e confidencialidade.

Segurança Física e do Ambiente

Em se falando de segurança física e do ambiente deve existir na XPTO um controle de acesso físico às diversas áreas da empresa. Para tanto é necessária uma prévia definição dos níveis de segurança para cada área da empresa e a consequente delimitação das barreiras de segurança física, explanadas nos parágrafos seguintes.

Na portaria da XPTO existirá um controle de acesso no qual os alunos matriculados somente poderão entrar com a devida utilização de carteirinha de identificação. A carteirinha possuirá tarja magnética que guardará as informações do aluno bem como do curso e turma que está matriculado.

Alunos não matriculados deverão identificar-se juntamente ao segurança, funcionário de empresa terceirizada, que encaminhará o mesmo à recepção ou fará com que o mesmo aguarde nas cadeiras do hall de espera, de acordo com a informação passada a ele pela recepção.

Apenas um funcionário treinado e devidamente autorizado pode acessar a tesouraria da empresa. Deve existir um sistema de videomonitoramento 24 horas para este setor, onde está o cofre da empresa XPTO. O mesmo vale para a sala de TI e o data center da empresa. Nesses três últimos setores, deve existir sistema de porteiro automático, com desbloqueio de trava mediante o uso de senha. A porta também pode ser aberta por algum funcionário que esteja dentro dela, para permitir a entrada solicitada por outro funcionário. Alunos não podem ter acesso a sala de TI ou tesouraria.

A XPTO deve seguir todas as normas impostas pelo corpo de bombeiros, fato inclusive necessário para a obtenção de alvará de processamento. Quanto ao risco de vazamentos de água, o que deve ser feito é o isolamento dos equipamentos do data center em referência a encanamentos, de modo que não passem pelas paredes da sala onde está o data center, ou ainda dentro dela, nenhum tipo de

encanamento.

Não será proibido que alunos ou colaboradores adentrem a escola munidos de equipamentos de produção audiovisual, entretanto é vedado o registro em áudio ou vídeo, sem o devido consentimento e autorização por parte da diretoria, de toda e qualquer atividade dentro da XPTO, sejam essas atividades de sala de aula, laboratório ou ainda eventos extraordinários, tais como: festa de halloween, valentines day entre outras que forem ofertadas nas dependências da XPTO.

Quanto à segurança dos equipamentos de informática contra furtos, deve existir uma trava de segurança em aço de modo a prender todos os equipamentos e evitar que os mesmos sejam facilmente levados por pessoas mal-intencionadas. Todas as janelas devem possuir grades para proteção contra invasões.

Não será permitido o consumo de alimentos, sucos ou refrigerantes dentro dos laboratórios ou sala de aula, salvo exceções, como em festas e eventos promovidos pela XPTO. Quanto à precaução contra cortes de energia todos os equipamentos deverão estar ligados a nobreaks.

Todo o cabeamento da XPTO será estruturado, com a utilização de calhas e armários em cada ambiente: recepção, tesouraria, sala de aula etc, de modo a prevenir interceptação do tráfego nos cabos como também o rompimento por vandalismo dos mesmos. Nenhum equipamento pertencente à empresa pode ser retirado de seu local sem o devido consentimento do responsável pelo mesmo em comum acordo com seu superior direto.

Todos os equipamentos de informática terão manutenções periódicas do tipo preventivas, com limpeza de dados desnecessários, atualização de aplicativos diversos e também a limpeza do hardware em si, com reaplicação de pasta térmica nos processadores a cada seis meses, de modo a garantir uma maior longevidade para os computadores da empresa.

Segurança em Recursos Humanos

O quesito da segurança em recursos humanos da XPTO, será divididos em três etapas: Antes da contratação, durante a contratação e encerramento da contratação.

Antes da contratação, teremos que tomar bastante cuidado em quem iremos contratar, pois como sabemos, o elo mais fraco de uma empresa é o ser humano, ele pode tanto ser envolvido em alguma engenharia social, como pode furtar ou danificar dados e informações. Então, antes mesmo de contratar, todos já devem saber quais as responsabilidades que serão atribuídas para tal cargo, tão importante quanto, o candidato, além de ciente da missão, da visão, dos princípios e valores da empresa XPTO, ele também tem que estar de acordo.

Importante que todos os candidatos, fornecedores e terceiros, assinem um acordo sobre seus papéis e responsabilidades pela segurança da informação.

Durante a seleção, iremos analisar o histórico dos candidatos, na entrevista teremos a confirmação se o currículo dos candidatos estavam coerentes e os selecionados farão um teste prático, pois dessa forma nos certificarmos melhor da capacidade de cada um, referente ao ambiente de trabalho e pressão do mesmo, a XPTO tem que contratar funcionários eficientes e preparados.

Agora estamos na segunda etapa, durante a contratação, nesta etapa iremos ter a certeza, que os contratados, sabem lidar com as ameaças e preocupações relativas à segurança da informação, com o objetivo de seguir a política de segurança da informação da XPTO dessa forma, diminuindo o risco humano. Vale ressaltar, que todos os funcionários da XPTO, receberão um nível avançado de conscientização, educação e treinamento nos procedimentos de segurança da informação e no uso correto dos recursos de processamento da informação, para não ferir e nem violar, a política de nossa empresa.

Lembrando que são todos os funcionários que receberão treinamentos e ficarão a par das políticas e das atualizações da XPTO, até porque nós somos uma equipe, e quanto mais falarmos a mesma língua e tivermos o mesmo objetivo e foco, mais sucessos teremos juntos.

A XPTO, também terá um processo disciplinar, ocorre quando algum funcionário, comete algum deslize, e fere de alguma forma a política de informações da nossa empresa. A priori chamaremos atenção, e daremos uma advertência no funcionário, mas agora ele ficará com uma chamada, o erro voltando a se repetir, poderá ser o último do mesmo. O objetivo é usar o processo disciplinar, como uma sanção, para evitar que os funcionários, fornecedores e terceiros violem os procedimentos e a políticas de segurança da informação, e quaisquer outras violações na segurança.

E por último, mas não menos importante, está o encerramento da contratação. Neste tópico iremos explicar quais procedimentos a XPTO tomará no desligamento do funcionário. Este tópico tem o objetivo de garantir que o funcionário se desligue da XPTO, de forma organizada e ordenada. A função de Recursos Humanos é o responsável pelo processo global de encerramento e trabalha em conjunto com o gestor responsável pela pessoa que está saindo, para gerenciar os aspectos de segurança da informação dos procedimentos pertinentes.

Neste procedimento de desligamento do funcionário com a XPTO, tem a devolução de ativos, que seria como o nome já diz, todos os funcionários, fornecedores e terceiros que tenham se desligado conosco, devolvam todos os ativos da organização que estejam em sua posse, após o encerramento das atividades, do contrato ou acordo. Importante salientar, se caso o funcionário tenha conhecimento de que seu trabalho é importante para as atividades que são executadas, este conhecimento deverá ser documentado e transferido para a XPTO.

E por fim, e último, ato do desligamento, será a retirada dos direitos de acesso dos funcionários. É importante sempre que possível, se o funcionário que

sair, for responsável por algum setor, que ele possa treinar algum outro, para o substituir, mas é claro que isto depende da forma que se deu o desligamento do mesmo. Quando o funcionário se desligar da XPTO, ele não terá mais vínculo contratual, com isso, ele também não terá mais acesso ao sistema, dessa forma se concretizando o desligamento.

Gerenciamento das Operações e Comunicações

O gerenciamento das operações e comunicações na XPTO, vai servir para garantir a operação segura e correta dos recursos de processamento da informação. Estes procedimentos terão que ser documentados e serão preparados para as atividades de sistemas associadas e recursos de processamento e comunicação de informações, os tópicos separados e trabalhados vão ser: Geração de cópias de segurança, manutenção de equipamentos, tratamento de mídias, segurança e gestão do tratamento das correspondências e das salas de computadores.

Gerenciamento da segurança em redes, tem como objetivo garantir a proteção das informações em redes e a proteção da infra-estrutura de suporte da XPTO. Para manter a segurança das informações que trafegam em uma rede, ela será controlada e monitorada regularmente e os acontecimentos serão registrados devidamente e sem falta. Na nossa rede terá sistemas como o firewall e também uma honeypot, elas são capazes de realizar o controle e o monitoramento.

Cópias de segurança, conhecido como backup, é um dos itens mais importantes e que de certeza tem que ter, tem como objetivo manter a integridade e disponibilidade da informação e dos recursos de processamento da informação. Bom ressaltar que na XPTO, todas as cópias de seguranças sempre que geradas, serão sempre testadas. As cópias sempre ficarão em uma localização remota, a uma distância suficiente para escapar dos danos de um desastre ocorrido no lugar principal, sempre quando houver informações sigilosos, usaremos a encriptação.

Tratamento de mídias, tem como objetivo prevenir contra a divulgação não autorizada, modificação, remoção ou destruição dos ativos. Segurança da documentação do sistema, sempre que possível, será protegida contra acessos não autorizados. A documentação dos sistemas sempre terá que estar guardado em algum lugar seguro; Nenhuma pessoa que não tenha autorização chegará perto dos documentos.

Descartes de mídias, todas as mídias da XPTO, que não forem mais ser utilizadas, deverão ser descartadas, por meio de procedimentos formais, estes auxiliará para um descarte seguro, dessa forma minimizando o risco de vazamento de informações sensíveis para pessoas não autorizadas. As mídias que contém informações sensíveis deverão ser descartadas e destruídas de forma segura, através da trituração ou incineração.

Troca de informações, tem o objetivo de manter a segurança na troca de informações e softwares internamente à organização e com quaisquer entidades

externas. Lembrar aos funcionários que eles não devem manter conversas confidenciais em lugares públicos, escritórios abertos ou locais de reunião que não disponham de paredes à prova de som. A troca de informações na XPTO, podem ocorrer através do uso de correios eletrônicos, fax, voz e vídeo.

Porém as informações podem ser comprometidas pelo motivo de falta de conscientização, de políticas ou de procedimentos no uso de recurso de troca de informações.

Comércio eletrônico, neste tópico o objetivo é fazer com que as informações contidas no mesmo, sejam protegidas de atividades fraudulentas, disputas contratuais e divulgação e modificações não autorizadas. A XPTO terá processos de autorização com quem pode determinar preços, emitir ou assinar documentos-chaves de negociação. É bom ressaltar que neste tópico a segurança tem que ser muito reforçada, pois além de ter muitos riscos, qualquer erro poderia ser fatal, com perdas de dados e danificações tanto para nossa empresa, quanto para os clientes. Temos que enfatizar novamente, principalmente neste caso, a proteção de dados é muito importante.

Monitoramento,na XPTO haverá monitoria, terá o objetivo de detectar atividades não autorizadas de processamento de informação, com isso o sistema será utilizado para checar a eficácia dos controles adotados e para verificar a conformidade com o modelo de política de acesso. O nível de monitoramento individual, será dado através de uma análise/ avaliação de riscos.

Nosso sistema também terá uma proteção das informações dos registros log, ele será protegido com o principal objetivo contra a falsificação e o acesso não autorizado. Alterações dos tipos de mensagens que são gravadas, arquivos de registros sendo editados ou excluídos.

Controle de Acesso

É o conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso. O controle de acesso a todos os serviços e informações poderá ser realizado por meio de cadastro e recadastro formal.

O conceito de controle de acesso baseia-se em dois princípios:

Separação de responsabilidades: Implica na separação de um determinado processo de modo que cada parte possa ser realizada por uma pessoa diferente,isto obriga os colaboradores a interagir para concluir um determinado processo, diminuindo as chances de fraudes.

Privilégios mínimos: Implica na concessão apenas dos privilégios mínimos necessários para que uma pessoa realize suas atividades, evitando o conhecimento de outras possibilidades, que eventualmente poderiam levar a incidentes de

segurança da informação.

A política de controle de acesso deve abranger pelo menos os seguintes temas:

1. Definição dos requisitos de negócio para controle de acesso;
2. Gerenciamento dos acessos pelos usuários;
3. Definição das responsabilidades dos usuários;
4. Controle de acesso à rede;
5. Controle de acesso ao sistema operacional;
6. Controle de acesso à aplicação e à informação;
7. Computação móvel e trabalho remoto.

Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Essa parte visa garantir que a segurança é a parte importante dos sistemas de informação, essa norma orienta tanto a direção quanto a definição dos requisitos para obter segurança no sistema, nesta norma também é incluso medidas preventivas contra processamento incorreto das aplicações, uso de controles criptográficos, além de fornecer diretrizes para a segurança dos arquivos de sistema, segurança em processos de desenvolvimento e suporte, e gestão de vulnerabilidades técnicas.

A segurança dos dados e informações em sistemas é um dos mais importantes objetivos de um sistema de segurança da informação, pois os procedimentos de desenvolvimento destes sistemas são uma questão vital para a segurança, a política de desenvolvimento de sistemas é o mecanismo para garantir estes resultados, mantendo em sigilo a CID da empresa.

A aquisição de sistemas possibilita o surgimento de diversas vulnerabilidades, um exemplo é a utilização de códigos abertos disponibilizados por comunidades é um dos perigos muitas vezes ignorados, a política de sistemas precisa garantir a diminuição destas vulnerabilidades.

O desenvolvimento e manutenção de sistemas também contém diversas vulnerabilidades, se não houver uma política explícita que oriente ao funcionário este desenvolvimento, vulnerabilidades poderão ser introduzidas no levantamento de requisitos, na construção do projeto, e na implementação do sistema, podendo ocasionar problemas futuramente.

A PSI deve se preocupar com os seguintes assuntos;

1. Definição dos requisitos de segurança para sistemas;

2. Processamento correto nas aplicações;
3. Controles criptográficos;
4. Segurança dos arquivos de sistema;
5. Segurança em processos de desenvolvimento e suporte;
6. Gestão de vulnerabilidades técnicas.

Gestão de Incidentes de Segurança da Informação

Controle

Evidências coletadas, armazenadas e apresentadas em conformidade com as normas
Uma ação de acompanhamento após um incidente de segurança da informação envolve uma ação legal

Diretrizes para implementação

São elaborados e respeitados procedimentos interno, a fim de buscar evidências para ações disciplinares
Admissibilidade da evidência: se a evidência pode ser ou não utilizada como prova
Importância da evidência: certeza das evidências e qualidade delas
Algum requisito aplicável sejam demonstradas por uma caminho certo de evidência
Manter de forma segura pessoa que encontrou ou testemunhou a descoberta,
Manter data e hora e documentos originais salvos e seguros.
Mídias eletrônicas fazer mais de uma cópia para garantir disponibilidade
Envolver um advogado ou a polícia tão logo seja constatada a possibilidade de processo jurídico.

Gestão de Continuidade de Negócio

Interrupção ou falha de processos críticos Plano de continuidade.
Assegurar disponibilidade da informação no nível requerido e na escala de tempo requerida. Identificar todas as responsabilidades e procedimentos da continuidade do negócio
Identificação de possíveis perdas de informações em níveis aceitáveis
Implementação dos procedimentos que permitam a recuperação e restauração
Procedimentos operacionais para recuperação de serviços
Qualificar pessoas para procedimentos para processos em momentos de gestão de crise
Atualização de teste procedimentos
Ambientes alternativos com nível de controles de segurança implementados,
Nestes locais seja equivalente ao ambiente principal.

Conformidade

Com requisitos legais a fim de evitar quaisquer obrigações estatutárias, regulamentares ou contratuais

-identificação da legislação aplicável, controle para que todos os requisitos estatutários, regulamentares e contratuais pertinentes,
Organizar para atender esses requisitos, sejam explicitamente definidos e documentos mantidos e atualizados para cada sistema
-direito de propriedade intelectual, divulgar uma política de conformidade com direitos de propriedade intelectual que define o uso legal de produtos e software e de informação
Adquirir software de fontes de reputação para não violar nenhum direito,
Conscientizar para proteger os direitos de propriedade, notificar pessoas que violarem
-proteção de registros organizacionais, categorizar em tipos de registros tais como registro contábeis,
Base de dados, transações, auditoria e procedimentos operacionais
-proteção de dados e privacidade de informações pessoais, manter privacidade e proteção de dados da organização, comunicar a todas as pessoas envolvidas no processo
-prevenção de mau uso de recursos de processamento da informação, convém que a direção aprove o uso de recursos de processamento
da informação ,este recursos devem ser somente utilizados para assuntos relacionados ao negócio
-regulamentação de controles de criptografia, restringir a importação ou a exportação de hardware ou software