1. Descreva alguns exemplos de desperdícios e de erros num ambiente de SI, suas causas e as possíveis soluções.

Contrato de licenças de software de forma desorganizada – Não é feito um estudo correto antes de efetuar o contrato, a solução seria validar onde e quando esse software realmente será necessário utilizar.

Não automatizar tarefas simples – O responsável por essas tarefas não ter a visão de automatizar os passos simples, a solução seria verificar quais processos existem a possibilidade de automatizar para ganhar tempo e recurso.

1. Explique os tipos e os efeitos dos crimes praticados por intermédio do computador juntamente com as medidas para sua prevenção.

Acesso e uso ilegal - O hacker é uma pessoas interessada em tecnologia da informação e que direciona seu tempo para aprender a usá-la. Um hacker criminoso, também conhecido com cracker, é um individuo com experiência em computação, que tenta acessar sistemas computadorizados sem autorização ou de forma ilegal.

Medidas de prevenção:

Instalar um forte recurso de autenticação do usuário e de criptografia no seu firewall

Instalar novos recursos em termos de segurança

Alteração ou destruição de dados - Os tipos mais comuns são os vírus e os worms, ou seja, programas que, quando executados, irão causar destruição, interrupção ou ocasionar erros no processamento. Um vírus é um programa que se anexa por si próprio a outros programas, enquanto um worm funciona como um programa independente, duplicando seus próprios arquivos até interromper a operação de redes e sistemas. Os tipos mais comuns de vírus são: a) Vírus de Aplicativo – infecta arquivos executáveis, como os programas de processamento de texto. b) Vírus de Sistema – infecta, em geral, os programas do sistema operacional ou outros arquivos de sistema.

c) Vírus de Macro – usa a linguagem de programação da própria aplicação para se autodistribuir. Diferentemente dos anteriores, os vírus de macro não infectam programas, somente documentos.

Medidas de prevenção:

Restringir o acesso físico ao servidor e configurá-lo de modo que a invasão de um servidor não comprometa a rede por inteiro

Furtos de informações e de equipamentos - O uso de “farejadores” de senha (password sniffers) é uma abordagem, na qual um pequeno programa, escondido numa rede ou num sistema, registra as senhas e os números de identificação.

Medidas de prevenção:

Instalação de softwares confiáveis e antivírus potentes, mantendo sempre atualizado.

Pirataria de software e na Internet - As cópias ilegais são chamadas de cópias piratas; o ato de duplicar ilegalmente é chamado de pirataria de software. Pirataria na internet envolve obter acesso de forma ilegal e, assim, fazer uso dos recursos.

Medidas de prevenção:

Efetuar download de softwares sempre na fonte original, efetuando o pagamento quando necessário.

Esquemas fraudulentos por computador - Nestes casos, o golpista oferece transações envolvendo bens imóveis, fraudes bancárias, loterias por telefone, ações, bem como alternativas de evitar pagamento de impostos, entre outros esquemas do tipo “fique rico rapidamente”.

Medidas de prevenção:

Não sair clicando em links duvidosos, caso esteja desconfiado, na primeira tentativa digite sua senha incorretamente para identificar o retorno do site, caso apresente alguma mensagem de sucesso, o site não é válido, pois não está realmente validando suas informações.

1. Como o computador pode ser objeto de um crime?

Através do seu uso, o usuário pode sofrer ou praticar um ataque hacker, roubando e ou distribuindo informações sigilosas, atualmente existe a LGPD (Lei Geral de proteção de dados) com intenção de boas práticas para minimizar esses vazamentos.

1. O que é pirataria de software e por que ela é tão comum?

A pirataria é uma prática comum entre os usuários da web, que varia de áudios e vídeos até softwares e sistemas operacionais. O crime é caracterizado pela distribuição, cópia ou venda não autorizada de qualquer mercadoria que possua direitos autorais. É comum pois o preço final para o usuário acaba sendo muito alto.