## 1.Procedimentos operacionais e responsabilidades

A fim de manter efetivos o gerenciamento e o controle de TI de uma organização, é importante documentar os procedimentos para a operação dos equipamentos e atribuir a responsabilidade das atividades de trabalho, tais como a forma como os computadores são ligados e desligados, fazer backups, manutenções, processar correspondências entre outras.

Um procedimento operacional inclui, por exemplo:

- Como lidar com a informação
- Como, quando e quais backups são feitos
- Pessoas de contato no caso de um cliente
- Gestão de trilhas de auditoria e arquivos de log

A principal finalidade de um procedimento operacional é assegurar que não haja mal-entendimentos acerca da forma no qual o equipamento deve ser operado. Não importa se for um robô de solda, um programa que controla uma estação elétrica ou um programa de contabilidade. As trilhas de auditoria e os arquivos de log do sistema mantém um registro de todos os eventos e ações que ocorrem no sistema e na rede. Esses arquivos são armazenados em um local seguro e não podem, em teoria, ser modificados. No caso de problemas, esses arquivos são muitas vezes cruciais para a descoberta do que deu errado.

## 2.Gerenciamento de mudanças

A implementação de uma mudança pode levar a uma situação de “beco sem saída”. Tanto implementar quanto não implementar uma mudança envolve risco. Essa situação pode ocorrer no caso de uma vulnerabilidade conhecida. Não instalar uma atualização necessária é um risco, à medida que a vulnerabilidade pode ser explorada e levar a interrupções na infraestrutura. Por outro lado, instalar a atualização também é um risco, uma vez que circunstâncias imprevisíveis podem levar a interrupções. O risco potencial de não instalar uma atualização de segurança é determinado pelo ISO (Information Security Officer), enquanto os riscos associados à mudança devem ser avaliados pelo gerente do sistema.

Se mudanças tiverem que ser feitas a serviços de TI e sistemas de informação, então elas devem ser cuidadosamente consideradas, de forma antecipada, e conduzida de forma controlada. No gerenciamento de serviços de TI e também na estrutura do ITIl, este processo é chamado de gerenciamento de mudanças.

O gerenciamento de mudanças coordena e monitora as alterações em sistemas. São frequentemente mudanças que foram planejadas de forma antecipada. Uma mudança tem consequências que devem ser compreendidas e preparadas com antecedência. O staff deve aprender a trabalhar com a nova versão. Formulários padrão devem ser modificados, e o pessoal da central de atendimento deve ser treinado para ser capaz de continuar ser cuidadosamente testado.

Sistemas de produção devem ser alterados apenas se houver razões substanciais para isso, tais como um risco aumentado para o sistema. Atualizar sistemas para a última versão do sistema operacional ou aplicação nem sempre é do interesse de uma empresa, uma vez que isso pode resultar em maior vulnerabilidade e instabilidade.

## 3.Gerenciamento da capacidade

É necessário identificar e monitorar os requisitos de capacidade dos sistemas de TIC das organizações, para prevenir interrupções indesejadas devido à falta de largura de banda, espaço em disco, alocação de memória e a capacidade de processamento. O gerenciamento da capacidade também é sobre definir e monitorar desempenho e espaço de bancos de dados e consumo de memória. Um cuidado especial deve ser dado aos sistemas críticos. A infraestrutura do ITIl á um processo definido para o gerenciamento da capacidade.

## 4.Proteção contra malwares

### 4.1 Malware

Malware é a combinação das palavras “malicious” e “software” e se refere a softwares indesejados, tais como vírus, worms, cavalos de Troia (trojans) e spyware. Uma medida padrão contra malware é usar antivírus e firewalls. Entretanto, está ficando cada vez mais claro que um antivírus sozinho não é suficiente para parar um malware. Uma das principais razões para o surto de vírus são as ações humanas. Uma infecção de vírus pode muitas vezes ocorrer através de um usuário que abre um anexo em um e-mail, que contém mais do que apenas o jogo, documento ou imagem prometidos, mas também contém um vírus.

### 4.2 Phishing

Phishing é uma forma de fraude na Internet. Tipicamente, a vítima recebe um e-mail pedindo para ele ou ela verificar ou confirmar uma conta junto a um banco ou provedor de serviços. Algumas vezes, mensagens instantâneas são usadas e até contatos telefônicos já foram tentados. É difícil apanhar os autores de phishing. Usuários de Internet devem permanecer particularmente vigilantes e não devem nunca responder a um pedido por e-mail para transferir dinheiro ou enviar informações pessoais, tais como número de conta de banco, códigos PIN ou detalhes do cartão de crédito.

### 4.3 Spam

Spam é o nome usado para se referir a mensagens indesejadas. O termo é normalmente usado para e-mails indesejados, mas as mensagens publicitárias indesejadas em websites também são consideradas spam. Os custos do spam são passados para o destinatário. Um filtro de spam pode aliviar um pouco esse fardo. Há também algumas outras coisas que os usuários de computador podem fazer para combater o spam. Uma delas é nunca responder uma mensagem de spam, uma vez que assim você confirma para quem enviou o spam que seu e-mail funciona e o spam sem dúvida irá aumentar. Além disso, não encaminhe mensagens de spam e não distribua endereços de e-mail.

## 4.4 Vírus

Um vírus é um pequeno programa de computador que propositalmente se replica, algumas vezes de forma alterada. As versões replicadas do vírus original são, em virtude dessa definição, também vírus. Para que o vírus se espalhe, ele depende de portadores que contenham um código executável. Assim que o portador é ativado, o vírus busca por novos portadores adequados e tenta infectá-los. O vírus só pode se espalhar fora do alcance do sistema infectado se um usuário transferir arquivos do sistema infectado para um novo sistema.

Os portadores eram tradicionalmente só programas, mas atualmente, os documentos também podem agir como hospedeiros para um vírus, uma vez que eles possuem cada vez mais códigos executáveis, tais como marcos, VBScript ou ActiveX. Na grande maioria dos casos, os vírus são equipados com uma carga útil que contém todas as tarefas que não sejam aquelas necessárias para a replicação. Essa carga é geralmente, mas não necessariamente, sempre, destrutiva.

Medidas protetivas incluem:

- Garantir que há um antivírus no servidor de e-mails e nos computadores individuais do local de trabalho. Sempre ter um antivírus com as definições atualizadas.
- Assegurar que o assunto vírus esteja incluído em uma campanha de conscientização de segurança
- Assegurar que esse assunto esteja incluído na política de segurança da informação da organização
- Assegurar que existam formas efetivas de reportar incidentes e bons procedimentos de acompanhamento

## 4.5 Worm

Um worm é um pequeno programa de computador que propositalmente se replica. Os resultados da replicação são cópias da programação original para outros sistemas, fazendo uso de equipamentos da rede de seu hospedeiro. Embora as diferenças entre vírus e worms estejam ficando cada vez mais turvas, eles ainda têm uma série de características distintas. Um vírus pode atacar seu hospedeiro por meio de diferentes portadores e infectar novos portadores transferindo código ativo para esses novos portadores.

Um worm, por outro lado, não depende de um usuário para se espalhar, assim que o worm é ativado, ele consegue se espalhar automaticamente. É isso que habilita os worms a infectar grandes áreas em um curto período de tempo. As duas similaridades mais importantes são a dependência de um código executável no portador e o uso de uma carga útil para realizar tarefas secundárias, usualmente destrutivas.

Medidas protetivas includem:

- Assegurar que haja um antivírus no servidor de e-mail e nos computadores individuais do local de trabalho. Sempre ter um antivírus com definições atualizadas.
- Uma vez que worms podem ser descobertos na rede, usar uma ferramenta de monitoramento de rede
- Assegurar que o assunto “worms” esteja incluído em uma campanha de conscientização de segurança
- Assegurar que este assunto esteja incluído na política de segurança da informação da organização
- Assegurar que existam formas efetivas de relatar incidentes e bons procedimentos de acompanhamento

### 4.6 Cavalo de Troia

Um cavalo de Troia, ou trojan, é um programa que, além da função que aparenta desempenhar conduz propositalmente atividades secundárias, imperceptíveis pelo usuário do computador, o que pode prejudicar a integridade do sistema infectado. Assim como o cavalo de Troia real, um trojan se apresenta como algo útil, mas quando ativado pelo usuário, pode conduzir todo tipo de atividade indesejada em segundo plano. A carga útil de um cavalo de Troia frequentemente instala um backdoor, através do qual pessoas desconhecidas podem ganhar acesso não autorizado ao sistema infectado. Outra atividade frequente dos trojans é enviar informações confidenciais do sistema infectado para outro local, onde elas podem ser coletadas e analisadas. A diferença mais notória com relação aos vírus e worms é que os cavalos de Troia não podem se autoreplicar. Como resultado, cavalos de Troia são normalmente capazes de realizar seu trabalho sem serem percebidos por um longo período de tempo.

Medidas protetivas incluem:

- Assegurar que haja um sistema de varredura contra cavalos de Troia e/ou vírus no servidor de e-mail e nos computadores individuais. Assegurar que o antivírus seja atualizado regularmente
- Assegurar que o assunto “cavalos de Troia” estejam incluído em uma campanha de conscientização de segurança
- Assegurar que o assunto esteja incluído na política de segurança da informação da organização. As consequências dos cavalos de Troia também podem ser descobertas pelos administradores de rede com ferramentas de monitoramento
- Outra contramedida é o uso de um firewall pessoal no próprio local de trabalho, a fim de detectar tráfego suspeito na rede
- Garantir que existam formas efetivas de reportar incidentes e bons procedimentos de acompanhamento

### 4.7 Hoax

Um hoax é uma mensagem que tenta convencer o leitor de sua veracidade e depois busca persuadi-lo a realizar uma determinada ação. A propagação de um hoax depende dos leitores deliberadamente enviarem a mensagem para outras vítimas em potencial, que também podem fazer o mesmo. A identificação do hoax é o primeiro passo para parar sua propagação. A carga útil de um hoax não é técnica por natureza, é psicológica. Ao jogar com a emoção das pessoas, o hoax tenta persuadir o leitor a enviá-lo a outras pessoas. Este é quase sempre o propósito de um hoax, embora possa, em certas ocasiões, tentar convencer a pessoa a depositar dinheiro, fornecer informação pessoal ou similares. Correntes de e-mail são a mais significativa e bem sucedida forma de hoax.

Medidas protetivas incluem:

- Assegurar que haja antivírus no local de trabalho e uma solução antispam no servidor de e-mail. Um hoax frequentemente contém textos que podem ser reconhecidos por tais soluções
- Assegurar que o assunto “hoaxes” esteja incluído em uma campanha de conscientização de segurança
- Assegurar que o assunto esteja incluído na política de segurança da informação da organização
- Garantir que existam formas efetivas de reportar incidentes e bons procedimentos da organização
- Garantir que existam formas efetivas de reportar incidentes e bons procedimentos de acompanhamento

## 4.8 Bomba lógica

Uma bomba lógica é um pedaço de código que é construído em um sistema de software. Este código executará uma função quando condições específicas forem atendidas. Isso nem sempre é usado para propósitos maliciosos. Um programador, pode produzir um código que destrói arquivos uma vez que ele saia da rede da empresa. Vírus e worms frequentemente possuem bombas lógicas, que normalmente têm um atraso embutido para a execução do vírus e propagação do worm. Para um software escrito por pessoal da empresa, ou sob contratos com terceiros, assegurar uma revisão do código seja feita por outra parte.

## 4.9 Spyware

É um programa que coleta informações no computador do usuário e as envia para outra parte. O propósito disso é fazer dinheiro. O spyware não tenta propositalmente danificar o PC e/ou o software nele instalado, mas sim, violar a privacidade. Spyware pode, algumas vezes, ser reconhecido de diversas formas, por exemplo: o computador está mais lento que o usual; programas que você nunca iniciou, ou que você nunca viu antes, estão sendo executados no computador; as configurações do computador foram modificadas, podendo haver uma barra de ferramentas no seu navegador de Internet que antes não estava ali e agora não pode ser removida; todos os tipos de janelas pop-ups aparecem sem aviso ou ao abrir páginas da web.

Medidas protetivas incluem:

- Garantir que os softwares do local de trabalho sejam atualizados regularmente
- Ter scanners que inspecionam o registro do Windows em busca de chaves de registro suspeitas e inspecionam softwares instalados em busca de spyware. Às vezes programas de antivírus também podem detectar spyware.
- Usar um firewall pessoal a fim de detectar tráfego de rede suspeito, especialmente tráfego que sai do seu computador sem nenhuma razão.
- Assegurar que o assunto "spyware" esteja incluído em uma campanha de conscientização de segurança. O staff deve ter cuidado com perguntas estranhas nos e-mails, especialmente aqueles que tentam convencer o leitor a realizar determinadas ações
- Assegurar que o assunto esteja incluído na política de segurança da informação da organização
- Garantir que existam formas efetivas de reportar incidentes e bons procedimentos de acompanhamento

### 4.10 Botnets

Botnet é uma combinação das palavras robot e network. O termo é normalmente utilizado com uma conotação negativa ou maliciosa. Um botnet é uma coleção de programas conectados a outros programas similares, via Internet, a fim de realizar tarefas no computador de algumas pessoas. Esses programas podem se comunicar por meio de vários canais para realizar diferentes tarefas, tais como enviar e-mails de spam ou participar de um ataque distribuído de negação de serviço. É possível se tornar parte de um botnet clicando em um link em um e-mail ou em uma página web, ou abrindo um anexo inseguro de e-mail onde um malware está escondido.

Muitas vezes, malwares podem ser baixados sem qualquer noção do usuário. Quando um computador se torna um bot, é mantida uma conexão com um servidor de comando e controle, de onde o operador do botnet pode instruir todos os computadores comprometidos a realizar tarefas. Novas análises sobre tendências da web mostram que o número de sites suspeitos está aumentando imensamente, diariamente. Existem botnets com milhões de bots e muito esforço vem sendo feito para derrubar servidores de comando e controle

Medidas protetivas incluem:

- Garantir que os softwares do local de trabalho sejam atualizados regularmente
- Ter scanners que inspecionam o registro do Windows em busca de chaves de registro suspeitas e inspecionam softwares instalados em busca de worms. Às vezes programas de antivírus também podem detectar atividades de worms
- Usar um firewall pessoal a fim de detectar tráfego de rede suspeito
- Worms também podem ser descobertos na rede; ferramentas de monitoramento de rede estão disponíveis para isso
- Assegurar que o assunto "botnet" esteja incluído em uma campanha de conscientização de segurança. O staff deve ter cuidado com perguntas estranhas

nos e-mails, especialmente aqueles que tentam convencer o leitor a realizar determinadas ações. Websites suspeitos devem ser evitados; existe um software que indica em seu navegador de Internet quando um website pode ser inseguro
- Assegurar que o assunto esteja incluído na política de segurança da informação da organização
- Garantir que existam formas efetivas de reportar incidentes e bons procedimentos de acompanhamento

### 4.11 Rootkits

Um rootkit é um conjunto de ferramentas de software que são frequentemente usadas por um terceiro após ter obtido acesso a um sistema. O rootkit se esconde com profundidade no sistema operacional, possivelmente fazendo com que este se torne instável. É quase impossível remover um rootkit sem danificar o sistema operacional. Em termos gerais, os rootkits podem trabalhar em dois níveis: no nível do kernel e no nível do usuário.

Processadores modernos conseguem lidar com programas no modo de kernel e no modo de usuário, e essa diferença é fundamental: programas no modo kernel têm acesso a toda a área de memória, enquanto aplicações no modo usuário são limitadas a segmentos específicos da memória. Rootkits com estratégias de kernel podem, portanto, fazer quase tudo que quiserem na memória de trabalho. O propósito dessas ferramentas é ler, alterar ou influenciar os processos em execução, dados ou arquivos do sistema. Um rootkit ajuda o invasor a ganhar acesso ao sistema, sem o usuário perceber nada.

Existem rootkits para quase todos os sistemas operacionais. Os rootkits se tornaram mais publicamente conhecidos em 2005, quando veio à tona que a gravadora Sony/BMG introduziu rootkits por meio de seus CDs de música, a fim de instalar segurança contra cópias. No final de agosto de 2007, rootkits foram introduzidos novamente em produtos da Sony. Dessa vez foi para proteger cartões de memória. Um rootkit foi usado para prover melhor proteção, mas, infelizmente, não foi dada atenção suficiente para as consequências de aplicar essa controversa medida de segurança. Essa medida de segurança, na verdade, não foi desenvolvida pela Sony, mas pela empresa

FineArt Technology, de Taiwan. Rootkits são extremamente difíceis de detectar e infectam o sistema muitas vezes sem o usuário perceber nada. Eles podem se esconder e também se disfarçar enganando programas de detecção. O único propósito de um rootkit é criar e esconder arquivos, conexões de rede, endereços de memória e entradas de índice. Mesmo quando o rootkit é removido, as mudanças que fez no sistema permanecem inalteradas e são normalmente imperceptíveis. Em outras palavras, a única forma de ter certeza absoluta que um rootkit foi removido é formatar e reinstalar todo o sistema a partir do zero.

Medidas protetivas incluem:

- Garantir que os softwares do local de trabalho sejam atualizados regularmente

- Ter scanners que inspecionam o registro do Windows em busca de chaves de registro suspeitas e inspecionam softwares instalados em busca de rootkits. Às vezes programas de antivírus também conseguem detectar rootkits, entretanto, é recomendado utilizar ferramentas especiais que rastreiam e destroem rootkits.
- Usar um firewall pessoal a fim de detectar tráfego de rede suspeito; o software de rootkit pode fazer uso do tráfego da rede
- Rootkits utilizam capacidade do processador e memória interna. Mesmo que os rootkits estejam bem escondidos, existem programas que podem detectá-los
- Assegurar que o assunto "rootkit" esteja incluído em uma campanha de conscientização de segurança. O staff deve ter cuidado com perguntas estranhas em e-mails
- Assegurar que o assunto esteja incluído na política de segurança da informação da organização
- Garantir que existem formas efetivas de reportar incidentes e bons procedimentos de acompanhamento

## 5.Backup

O propósito de fazer backups, ou cópias reversas, é manter a integridade e a disponibilidade da informação e das instalações computacionais. As consequências da perda de informação dependem da idade da informação que pode ser recuperada a partir do backup. É importante, portanto, considerar o intervalo em que os backups são feitos. Quanto tempo podemos nos permitir recuperar novamente a informação que foi perdida ? É importante que o backup seja testado regularmente. Além de realmente fazer e testar os backups, também é necessário considerar como os backups são manejados. Os backups são retirados de prédios altamente seguros e depois colocados em armários destrancados ? Ou os backups são colocados próximos ao servidor com os dados originais ? Os dados são criptografados ? Por quanto tempo os backups são armazenados ? Isso atende aos requisitos legais de armazenamento.

## 6.Registro de monitoração

Com o aumento dos ataques de malware, e também com o mau comportamento, intencional ou não, de usuários, é necessário ter a capacidade de registrar eventos e produzir evidências. Para esse propósito, é essencial ter um bom registro

### 6.1 Registro de evento (log)

O registro de evento (log) é a coleção de atividades de sistemas e de usuários, exceções, falhas e eventos de segurança da informação. Ao coletar os logs de eventos é importante que você olhe para as informações coletadas; caso contrário, a coleta de logs é inútil. Tenha em mente que os logs devem ser mantidos em um local seguro e protegidos contra modificações ou exclusão das informações coletadas. Antes de começar a coletar os logs, pense sobre o que registrar, por quanto tempo manter os logs e quem deve acessar a informação. Para garantir que logs diferentes possam ser usados para investigar um evento de segurança, os relógios do sistema devem ser sincronizados com uma única fonte de referência de tempo. Tenha em

mente que arquivos de log contendo dados pessoais devem ser protegidos conforme as leis de privacidade.

## 6.2 Controle de software operacional

Software operacional é o software usado nos sistemas operacionais. Dentro de uma organização, a manutenção de softwares operacionais por usuários finais não deve ser permitida e só deve ser efetuada pelos operadores depois de testada. É importante pensar em uma estratégia de restauração caso algo dê errado ao atualizar os sistemas operacionais, mesmo após um bom teste

## 6.3 Gestão de vulnerabilidades técnicas

Uma vulnerabilidade é uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Uma vulnerabilidade caracteriza a ausência de proteção ou a fragilidade de uma proteção que pode ser explorada. Essa vulnerabilidade pode ser um serviço executando em um servidor, aplicações ou sistemas operacionais não corrigidos, acesso discado irrestrito via modem, uma porta aberta em um firewall, segurança física fraca que permite que qualquer pessoa entre em uma sala de servidor ou um fraco gerenciamento de senha em servidores e estações de trabalho.

## 6.4 Gerência de vulnerabilidades técnicas

Uma vulnerabilidade técnica é uma fraqueza em um sistema computacional que permite que alguém ataque o sistema computacional vulnerável. Existem muitas vulnerabilidades que são encontradas por hackers éticos ou por coincidência. Todo sistema operacional possui vulnerabilidades, às vezes conhecidas e às vezes desconhecidas pelo proprietário. É importante que, tão logo a vulnerabilidade seja conhecida, medidas apropriadas sejam tomadas para prevenir que atacantes explorem a vulnerabilidade.

Para vulnerabilidades desconhecidas, um processo de gestão de incidentes é necessário para garantir uma resposta apropriada no caso de uma violação. Para vulnerabilidades conhecidas, os fornecedores provavelmente fornecerão atualizações ou correções. Essas correções devem ser testadas e verificadas para garantir que o software operacional continue funcionando como planejado. Se não houver correção disponível, o risco pode ser minimizado adotando medidas de segurança, como, por exemplo, isolamento do sistema, adaptação de firewall e maior monitoramento.