www.ProjetodeRedes.kit.net

Universidade Federal de Pernambuco
Departamento de Informática
Mestrado em Ciência da Computação

Política de Segurança

Centro de Estudos e Sistemas Avançados do Recife

Patrícia Nunes Pereira
Ana Maria Gomes do Valle
Henrique de Barros Saraiva Leão

Índice

Prefácio

Em toda Política de Segurança faz-se necessário ter uma idéia clara daquilo que se quer defender, contra quem queremos defender e quais os entraves que essa política oferece para funcionamento normal do sistema. Uma Política de Segurança de uma empresa define as normas e procedimentos que melhor atendam ao propósito da mesma, minimizados os riscos com perdas e violações de qualquer um dos seus bens. Podemos assumir que todos os dados referentes a uma empresa fazem parte do seu patrimônio. Nosso objetivo ao desenvolver esta Política restringe-se à defesa das informações e sistemas computacionais de software e hardware da empresa.

Durante o desenvolvimento de uma Política de Segurança precisamos entrar em contato com os indivíduos na empresa responsáveis pelos dois papéis-chaves para coleta das informações necessárias: os administradores de sistemas (tecnologia aplicada), os diretores da empresa (negócio da empresa). Os demais funcionários são os reais usuários da política e não podem ser esquecidos quanto às suas necessidades de execução de tarefas – ou seja, estas tarefas não devem serem suprimidas em prol da implementação da política, sem que ao menos seja-lhe oferecido um caminho alternativo - e quanto às suas reais possibilidades de execução daquela política – por limitações culturais ou técnicas.

Importante lembrar que o contato com esses personagens precisa ser feito com razoável freqüência para que a política acompanhe as várias mudanças nos processos de negócio ou de cunho tecnológico: *uma Política de Segurança é específica para uma empresa e deve acompanhar o seu desenvolvimento.*

Uma Política de Segurança não pode estar restrita à nenhuma instância de uma provável implementação da mesma. Ela deve ser construída em forma de procedimentos capazes de serem executados independente da tecnologia aplicada.

Estes foram os conceitos que tentamos seguir ao longo deste projeto.

Agradecimentos

À Ana Cristina dos Santos
Aldo Segundo
Marco Antônio Carnut
Administradores de Sistemas da Rede CESAR

Evandro Curvelo da Hora
Pela sua contribuição em sala de aula

Fábio Queda Bueno da Silva
Pela orientação técnica e bibliográfica

Introdução

Com o objetivo de desenvolver uma política de segurança para a Rede do CESAR é de fundamental importância, que aspectos particulares da empresa sejam considerados.

Em primeiro lugar, o negócio da empresa deve ser levado em conta. O Centro de Estudos e Sistemas Avançados do Recife – CESAR - foi concebido para suprir a necessidade de uma maior interação entre o meio acadêmico, o meio empresarial e a sociedade em geral. Além dessa cooperação entre indústria e academia, trabalha na criação de uma nova geração de empreendedores , que compreende o valor da pesquisa e do investimento em tecnologia no sucesso empresarial.

Em segundo, a política de segurança deve ser de conformidade com políticas, regras, regulamentos e leis existentes , às quais a empresa já está sujeita. Particularmente, no caso do CESAR, que trabalha em parceria com outras empresas, órgãos de incentivo à pesquisa e instituições governamentais, seria inviável uma política que impedisse a comunicação entre o CESAR e as empresas que ele suporta.

Será necessário identificar e considerar esses pré-requisitos, quanto do desenvolvimento da política de segurança.

Em terceiro lugar, é necessário considerar implicações de segurança num contexto mais global. A política deve se preocupar com problemas de segurança local, assim como possibilidade de invasões por pessoas externas e também de funcionários da empresa causando danos ou invasões a redes e sistemas de terceiros.

Quem faz a política?

A criação da política deve ser um esforço associado do pessoal técnico e do pessoal administrativo, que tem o poder de fazer cumprir a política. Uma política que não pode ser implementada, nem cumprida, não é útil.

Desde que a política de segurança pode afetar a todos em uma empresa, tem que se tomar cuidado para se ter a certeza de que existe um certo nível de autoridade nas decisões. Embora um grupo particular possa ter a responsabilidade de fazer cumprir a política, um grupo de mais alto nível pode ter que confirmar e aprovar a política.

Quem é envolvido?

A política de segurança, para ser apropriada e efetiva, precisa ter a aceitação e o suporte de todos os indivíduos da empresa. É especialmente importante que os diretores da empresa dêem total apoio ao processo de concepção da política de segurança, caso contrário, há pouca chance de que ela surta efeito. A lista, a seguir, abrange as pessoas que devem ser envolvidas na criação e revisão dos documentos da política de segurança:

- Administrador local de segurança.
- Administrador de recursos de informática.
- Staff técnico de recursos tecnológicos.
- Times de resposta de incidentes de segurança.
- Representantes de grupos de usuários afetados pela política de segurança.

Responsabilidades

O elemento chave para uma política de segurança é a de se ter a certeza de que todo mundo tem conhecimento de suas responsabilidades para manutenção da segurança.

Uma política de segurança não pode prever todas as possibilidades. Contudo pode garantir (assegurar) que, para cada tipo de problema, existe alguém designado para tratar com ele. Devem existir níveis de responsabilidade associados com a política de segurança. Em um nível, cada usuário de um recurso computacional deve ter a responsabilidade de proteger sua conta. Quando um usuário permite que sua conta seja comprometida, cresce a chance de serem comprometidas outras contas ou recursos.

Gerentes de sistemas podem formar outro nível de responsabilidade. Eles devem ajudar a garantir a segurança do sistema de computação. Gerentes de rede podem ainda pertencer a outro nível.

Comunicação da política de segurança

A política de segurança, para se tornar efetiva, deve ser comunicada aos usuários do sistema e ao pessoal da manutenção do mesmo. Todos devem assinar um termo indicando que leram, entenderam e concordaram em obedecer à política. É importante também destacar, que a realização de um forte treinamento com usuários, administradores e demais indivíduos envolvidos e/ou afetados pela política de segurança, constitui-se em medida fundamental para o sucesso e aceitação dos princípios estabelecidos por tal política.

Educação do usuário

Usuários devem ser alertados de como o sistema computacional espera ser usado e como protegê-lo de usuários não autorizados.

Todos os usuários devem ser informados sobre o que é considerado uso apropriado de sua conta. Isto pode mais facilmente ser feito, no momento que o usuário recebe sua conta, levando ao seu conhecimento os estatutos da política. Uma política de uso apropriado, tipicamente, dita coisas tais como de que forma a conta pode ser usada para atividades pessoais, de lazer ou ganho pessoal.

Análise de riscos

A análise de riscos serve para estimar o potencial de perdas associado às vulnerabilidades do sistema e quantificar o prejuízo que pode ocorrer, caso as ameaças se concretizem. O principal objetivo da análise de risco é tentar identificar proteções eficientes que reduzirão os riscos a um nível aceitável, de modo que se o site (sistema) for atacado, consiga sobreviver com os serviços essenciais.

A análise de riscos deve determinar:

- O que deve ser protegido.
- O que é necessário para garantir proteção.
- Como proteger.

Para isso, a análise de riscos segue duas fases:

- Identificação dos bens.
- Identificação das ameaças.

Identificação dos bens

Consiste em identificar todas as coisas que precisam ser protegidas. Em princípio os bens podem ser agrupados nas seguintes categorias:

- Hardware.

  CPUs, placas, teclados, terminais, estações de trabalho, computadores pessoais, impressoras, disk drives, linhas de comunicação, servidores, roteadores, hubs, switches, etc.

- Software.

  Programas-fonte, programas-objeto, programas utilitários, programas de diagnóstico, sistemas operacionais e programas de comunicação.

- Dados.

  Durante a execução, armazenados on-line, arquivados off-line, auditoria de logs, banco de dados, em trânsito nos meios de comunicação;

- Pessoas.

  Usuários, administradores, pessoal de manutenção;

- Documentação.

Programas, hardware, sistemas, procedimentos de administração local;

- Suprimentos.

Papéis, formulários, meios magnéticos.

No caso particular do CESAR, temos o seguinte:

Hardware

No apêndice, se encontra a descrição atual da rede do CESAR. Através dela podemos verificar a quantidade de estações e servidores pertencentes a empresa.

Software

Em termos de recursos de software, atualmente são utilizados os sistemas operacionais WindowsNT 4.0, Unix (AIX, Sun OS, Solaris e Linux). Além disso, existem ferramentas de desenvolvimento, tais como SGBD (Oracle), compiladores (Delphi), etc.

Identificação de ameaças

Consiste na identificação das ameaças aos bens. Isto ajuda a considerar de que ameaça estamos tentando proteger os bens:

- Acesso não autorizado

  Um acesso não autorizado seria o uso de conta de outro usuário para ganhar acesso ao sistema, ou uso de qualquer recurso computacional sem a prévia permissão. Um acesso não autorizado abre as portas para outras ameaças de segurança.

  O CERT (Computer Emergency Response Team) tem observado que os sites mais atacados são de universidades bem conhecidas, governamentais e militares.

- Acesso autorizado, mas de má fé

  Ocorre quando há um acesso permitido ao sistema, mas o seu usuário executa procedimentos de má fé, visando conseguir ganhos pessoais ou prejudicar a empresa com as informações adquiridas.

- Disponibilização não autorizada de informações
  Existem dois tipos de disponibilização de informações:
  1. **Voluntária** – ocorre quando há um roubo proposital, pode ocorrer através de vários meios, como correio eletrônico, invasão da rede da empresa, ou até mesmo através de meios não eletrônicos.
  2. **Involuntária** – impressão de documentos sigilosos em impressoras públicas, não destruição de cópias de informação confidencial, mensagens de correio eletrônico com destinatário errado, mensagens para listas eletrônicas.

A perda de informações pode causar danos irreparáveis para a empresa, projetos secretos, lista de clientes, licitações, etc.

- Negação de serviço

Computadores e redes fornecem valiosos serviços para seus usuários. Muitas pessoas contam com os serviços para desempenharem suas tarefas eficientemente. Quando estes serviços não estão disponíveis resulta numa perda na produtividade.

Negação de serviço vem de muitas formas e podem afetar usuários de muitas maneiras. Cada site deve determinar que serviços são essenciais e para cada serviço determinar como afeta o site se este serviço se tornar desabilitado.

- Outros problemas ou ameaças

Podem ocorrer outros problemas, como falhas e sobrecargas de energia, incêndios, roubos físicos, falhas de hardware, etc.

Política de Segurança

Escopo

Esta política se aplica a toda a rede do CESAR, incluindo servidores e as estações de trabalho que estejam conectados diretamente à rede interna, como também os computadores que acessem o CESAR através da Internet ou outra rede de comunicação de dados.

Níveis de Operação

Para efeitos de aplicação das regras da Política de Segurança e definição dos procedimentos que a implementem, ficam definidos os seguintes níveis de operação do sistema computacional do CESAR:

- **Rotina**: caracteriza a situação onde não existe suspeita de falhas na segurança do sistema, que deve estar sendo monitorado constantemente.

- **Emergência**: existe suspeita de algum ataque à segurança, com possíveis danos ao funcionamento seguro do sistema. Análise da informação de monitoração é realizada para confirmar a ocorrência do ataque.

- **Crise**: situação na qual um ataque à segurança está confirmado e ações devem ser tomadas para tratar o ataque e suas conseqüências.

Níveis de Confidencialidade da Informação

As informações armazenadas no sistema de computação do CESAR possuem três níveis de confidencialidade:

- **Pública**: informações que podem ser livremente lidas por qualquer usuário interno e através de outras redes (por exemplo, a Internet), por qualquer usuário externo. As informações públicas precisam ser protegidas somente de ataques à integridade e disponibilidade.

- **Privada**: informações que podem ser lidas por qualquer usuário interno, mas por nenhum usuário externo. Estas informações podem ser alteradas somente por alguns usuários internos autorizados. As informações privadas precisam ser protegidas de ataques externos à confidencialidade, integridade e disponibilidade, e de ataques internos à integridade e disponibilidade.

- **Confidencial**: informações que podem ser lidas e alteradas somente por um grupo restrito de usuários internos autorizados. Estas informações precisam ser protegidas contra ataques internos e externos à confidencialidade, integridade e disponibilidade.

Níveis de Criticidade dos Recursos

Os seguintes serviços e recursos, e as informações por eles armazenadas ou processadas, são considerados críticos:

- Windows NT
- *Domain Name Server* (DNS)
- Correio eletrônico
- Solaris 2.6
- Software de *firewall (Firewall –1)*
- Banco de dados Oracle
- Aplicativos corporativos
- Informações armazenadas nas cópias de segurança *(backup)*

Os demais recursos têm nível normal de criticidade.

Política de Acesso aos Recursos e Serviços

Acesso Físico aos Recursos

O cabeamento de rede do sistema deve ser protegido e seu acesso deve ser permitido somente em pontos sob o controle da administração de sistemas da empresa. É proibido ligar computadores, equipamentos de rede e analisadores de tráfego não autorizados pela administração da rede.

O acesso à sala de servidores por pessoal não autorizado, incluindo suporte externo realizado pelos fornecedores ou empresas terceirizadas, deve ser acompanhado por um administrador de sistema que tenha direito de acesso à sala.

As estações de trabalho e servidores que não estiverem localizadas na sala de servidores e que por esta razão têm acesso físico menos seguro, somente podem ser utilizadas através de uma conta de usuário com utilização de uma senha pessoal.

Os servidores localizados na sala de servidores não devem permitir acesso remoto a partir de computadores localizados em outros locais.

O usuário é responsável pela segurança de qualquer recurso computacional que estiver em seu poder fora ou dentro das premissas da empresa.

Acesso Lógico: Contas dos Usuários

Considerações Gerais

Somente funcionários e diretores do CESAR podem ter conta na rede. Os direitos destas pessoas são diferentes na rede NT e na rede Unix. Exceções devem ser autorizadas por escrito pela diretoria da empresa e as autorizações passarão a compor o *Log* de Segurança do sistema.

Segundo as necessidades da empresa, existem as seguintes categorias de contas e grupos com suas respectivas permissões:

- Administradores de rede – possuem permissão para todos diretórios;
- Contas de usuários – possuem diretórios com acesso individual;
- Grupos de projeto – possuem diretórios que são compartilhados pelos componentes do grupo e gerentes;
- Grupos de serviço (secretaria, imprensa, etc.) – possuem diretórios com permissão para os usuários pertencentes a este grupo

Podem existir também restrições de acesso específicas em subdiretórios localizados nas áreas compartilhadas. Por exemplo, apenas os gerentes de projeto podem acessar documentos de acompanhamento global do projeto localizados em um determinado subdiretório, porém os outros membros do projeto não podem.

Cada grupo possui diretórios no servidor nos quais apenas os membros do grupo tem acesso.

Em relação ao sistema operacional Solaris, a rede do CESAR possui as seguintes categorias de contas de usuários:

- Grupo do CESAR (funcionários, diretoria e desenvolvedores de projetos);
- Grupo para suporte.

Normalmente, apenas os usuários proprietários deveriam ter total permissão sobre seus arquivos. Os usuários pertencentes ao mesmo grupo, devem ter permissão apenas de leitura sobre o arquivo e os demais usuários não devem possuir nenhum direito sobre o arquivo.

Criação de Contas

Existe uma forma única de criação de contas de usuários, definida em procedimento próprio. Cada criação de conta deve ser documentada por escrito e fará parte do *Log* de Segurança. Esta documentação deve ser utilizada para dirimir dúvidas e reduzir erros que possam comprometer a segurança do sistema.

Ao criar uma nova conta, o administrador de sistemas criará também uma senha inicial para autenticação do acesso por parte do usuário. É **proibido** a criação de contas sem senha inicial. A senha inicial não pode ser "fácil" (no sentido definido pela lnternic RFC 1244) e não pode ser de conhecimento público.

Ao receber a sua conta e a senha inicial, o usuário receberá uma cópia da Política de Segurança e assinará o Termo de Compromisso. Ao assinar o termo, o usuário automaticamente declara estar ciente das regras e sanções impostas pela política.

Gerenciamento de Contas

Deve existir uma monitoração constante da utilização das contas dos usuários de todas as categorias. Esta monitoração levantará e catalogará no *Log* de Segurança as seguintes informações:

- Data, hora e local dos acesso.
- Recursos utilizados e por quanto tempo.
- Comandos executados.
- Tentativas de acesso as informações confidenciais.
- Informações confidenciais lidas, alteradas, copiadas ou removidas.

Ao fazer acesso a sua conta, o usuário deve ser avisado do dia, hora e local do seu último acesso, e quantos *logins* mal sucedidos foram feitos desde o último acesso. Esta informação deve ser observada com cuidado e, caso alguma anomalia seja detectada, deve ser informada à equipe de suporte.

As contas de usuários que não tiverem sido acessadas por um período superior a 03 meses serão automaticamente bloqueadas e seu acesso somente será permitido novamente através de solicitação por escrito de um diretor ou gerente de área. Esta solicitação passará a integrar o Log de Segurança do sistema.

Remoção de Contas

Usuários que tenham infringido maliciosamente as regras da Política de Segurança receberão uma advertência administrativa, e no caso de reincidência terão suas contas removidas da rede sem a cópia de segurança ou preservação dos dados contidos nela, com possibilidade de demissão.

Contas bloqueadas por um período superior a 06 meses serão removidas do sistema.

Contas de usuários que não são mais funcionários do CESAR ou cuja autorização explicita para abertura de conta não mais se aplicar, terão a sua conta removida do sistema.

As informações pertencentes a um usuário removido são de propriedade do CESAR, não podendo em hipótese alguma ficar de posse do usuário.

Usuários que tiverem suas contas removidas terão suas informações (documentos, arquivos e mensagens) guardadas *off-line* por um período máximo de 12 meses, para o caso de uma possível reabilitação da conta ou da necessidade da informação por parte da empresa. Exceção a esta regra são quanto aos usuários que não são mais funcionários do CESAR.

Reabilitação de Contas

A reabilitação de uma conta será realizada seguindo as mesmas regras definidas para a criação de contas

Caso o usuário reabilitado tenha suas informações guardadas, estas serão recuperadas e colocadas a disposição do usuário

Utilização Apropriada de Recursos

Os usuários podem utilizar somente a sua conta pessoal. A negligência ou ingenuidade de outros usuários em revelar sua conta ou senha não é considerada como consentimento para sua utilização. Conveniência de compartilhamento de arquivos ou impressoras não é razão suficiente para usuários compartilharem contas. Excetuando-se os casos onde seja necessário a criação de contas em conjunto para determinados projetos.

Os usuários não devem tentar modificar restrições associadas a suas contas pessoais e de outros usuários.

Os usuários são responsáveis pela utilização da suas contas. Eles devem se precaver contra acessos de outras pessoas às suas contas. A segurança individual da senha é de responsabilidade do usuário.

Os usuários são proibidos de modificar a configuração dos recursos e serviços, ou tentar interromper o funcionamento do sistema. As proibições desta regras incluem:

- alterar as proteções e restrições de acesso dos computadores, aplicações ou arquivos do sistema;
- tentativas de ultrapassar e alterar cotas do sistema;
- impedir outros usuários de utilizar determinado recurso, por alta utilização do mesmo, após ser dado um aviso de término desta atividade;
- utilizar programas para quebra ou captura de senhas;

- tentativa de adquirir privilégios maiores dos autorizados para a sua conta; acesso às informações para as quais o usuário não tem permissão.

Os usuários são responsáveis pela utilização de software e outros materiais em meio eletrônico de acordo com as leis de *COPYRIGHT* (e com as regras das licenças pertinentes). É proibida a cópia de *softwares*, documentação e materiais que possuem licença ou *copyright* sem a permissão por escrito do dono ou sem a licença apropriada.

É proibida a utilização ou instalação de software de jogos.

Em relação a utilização de correio eletrônico, é proibido:

- início ou retransmissão de correntes de mensagens eletrônicas, ou seja, mensagens que, a partir de um usuário, são retransmitidas para vários outros, causando um aumento exponencial da quantidade de mensagens na rede com o conseqüente aumento excessivo de utilização dos recursos do sistema;
- forjar ou tentar forjar mensagens eletrônicas;
- tentativas de leitura, remoção, alteração e cópia de mensagens eletrônicas de outros usuários;
- envio de mensagem indecorosas e obscenas para outros usuários internos ou externos;
- envio de material obsceno, indecoroso ou de cunho político ou racial, para outros usuários internos ou externos, mesmo com o consentimento destes;
- envio de mensagens não solicitadas (por exemplo: spam).

É proibido se ausentar da estação de trabalho ou servidor e manter a conta aberta, com acesso permitido a outros usuários. O usuário será responsabilizado por qualquer dano causado ao sistema por esta prática.

Usuários que, por qualquer motivo, não forem utilizar a sua conta por um período superior a 30 dias devem informar aos administradores de sistema, para que suas contas sejam temporariamente desabilitadas. Esta comunicação deve ser feita por escrito e passará a integrar o *Log* de Segurança. A reabilitação da conta se dará através de solicitação do usuário por escrito e também fará parte do *Log* de Segurança

Acesso Remoto

É proibida a existência e/ou utilização de acesso remoto via *modens* ou outras formas de acesso(por exemplo: backdoors) que não sejam pela lnternet ou através de Provedor de Acesso disponibilizado pelo CESAR. Não está sendo referido à forma de acesso via SSH.

Acesso à Informação Confidencial

As informações consideradas confidenciais devem ser protegidas ao máximo. Quando armazenadas na rede deve existir um controle de permissões e mecanismos de

criptografia que assegurem a sua confidencialidade. Para tanto as seguintes políticas são definidas:

Informações confidenciais devem ter uma documentação associada indicando o dono, data de criação, data da última modificação. tempo de vigência e permissões. As permissões devem indicar quais usuários podem ler, alterar e copiar o documento, o acesso indevido de qualquer dado que não possua esta documentação será de responsabilidade exclusiva do usuário a quem a informação pertence.

Informações e documentos confidenciais só podem ser armazenados em locais seguros e previamente definidos pela gerência de segurança. A apropriação indevida de qualquer informação confidencial que não esteja armazenada nestes locais será de responsabilidade exclusiva do usuário a quem a informação pertence.

É vetada a utilização de impressoras compartilhadas para impressão de documentos contendo informações sigilosas.

Às informações confidenciais contidas em qualquer mídia devem ser destruídas após sua utilização**.**

Ao enviar informação confidencial pelo correio eletrônico o usuário deve:

- criptografá-la ou utilizar qualquer outro mecanismo que torne a comunicação segura;
- verificar os destinatários para ter certeza de que são autorizados a receber a informação;
- verificar os membros das listas eletrônicas que são destinatárias da mensagem para ter certeza de que todos são autorizadas a receber a informação.

Um *log* de todos os acessos e tentativas de acesso às informações privilegiadas deve ser mantido no sistema.

Política de Autenticação de Acesso

A autenticação de acesso à rede é realizada através de senhas. As políticas definidas a seguir se aplicam as contas dos sistemas Windows NT .

A segurança através de sistemas baseados em senhas depende de mantê-las secretas. Para que o sistema de autenticação permaneça eficaz e para que as senhas não se tornem vulneráveis, dois grupos de políticas de senhas devem ser definidas; política de senhas iniciais, que rege a criação e manutenção da senha quando da abertura da conta, e a política de utilização da senhas.

Políticas de Senhas Iniciais

Ao abrir uma nova conta, uma senha inicial será gerada através de um processo automático que garanta que a senha não é facilmente adivinhada e não é conhecida por nenhum outro usuário.

Uma senha nova deve ser gerada para cada nova conta. Reutilização de senhas ou a utilização de uma senha padrão coloca sério risco a segurança do sistema.

É responsabilidade dos administradores de segurança do sistema gerar e cadastrar a senha inicial de cada usuário

É responsabilidade dos administradores de segurança informar ao usuário sua senha inicial. Isso deve ser feito com comunicação pessoal ao usuário evitando a exposição da senha em meios de comunicação eletrônicos ou não. Desta forma, a senha inicial não deve ser enviada por nenhum meio, exceto em casos excepcionais, onde os usuários estejam remotos, quando a comunicação (não puder ser pessoal) deverá ser feita por telefone.

Ao obter a sua senha inicial, o usuário receberá uma documentação explicando como realizar a troca de senhas de forma segura.

Ao fazer acesso pela primeira vez a sua conta, o usuário deve trocar a senha inicial por uma senha pessoal e confidencial. Esta senha deve possuir no mínimo 8 caracteres.

A geração de outra senha pelo administrador de sistemas (por exemplo, no caso do usuário esquecer a sua senha pessoal) deve seguir as mesmas regras das senhas iniciais.

Políticas de Utilização das Senhas

O sistema deve fornecer as ferramentas necessárias para que o usuário seja capaz de, pessoalmente, trocar a sua senha.

Os usuários devem trocar suas senhas pessoais periodicamente. A senha expira após 90 dias, obrigando desta forma ao usuário trocá-la

A senha trocada não pode ser igual as 6 últimas senhas anteriores.

Os usuários devem trocar a sua senha sempre que suspeitarem que violações à segurança podem ocorrer através da utilização indevida da sua senha.

Os usuários devem memorizar a sua senha. Guardar a senha por escrito em qualquer tipo de mídia ou local é uma falha grave de segurança e é expressamente proibido.

A descoberta da senha pessoal por outras pessoas, usuários ou não, deve ser imediatamente comunicada ao pessoal do suporte e a senha deve ser imediatamente trocada.

0 sistema irá permitir no máximo 10 tentativas de acesso ao sistema sem sucesso por erro no fornecimento da senha. Após a décima tentativa, a conta do usuário será automaticamente bloqueada por 30 minutos e a ocorrência será registrada no log de segurança.

O processo de criação de senhas deve seguir as normas definidas na RFC 1244.

As senhas para os sistemas Windows NT e Solaris devem ser diferentes.

Política de Privacidade da Informação

Apesar de respeitar a privacidade dos usuários do sistema, o CESAR tem o direito de auditar e monitorar, processos do sistema, tentativas (com ou sem sucesso) de acesso aos recursos da rede e do sistema computacional, utilização de tempo de CPU e/ou de largura de banda da rede, espaço em disco utilizado por programas, proteções e permissões de acesso a arquivos, utilização do sistema para envio de mensagens e arquivos, etc.

Apenas em situações de suspeita que algo errado pode estar acontecendo, os administradores de sistema do CESAR, podem inspecionar o conteúdo de mensagens e arquivos, inclusive podendo arquivá-los ou removê-los caso seja necessário para manter o funcionamento seguro do sistema. Este procedimento será realizado com autorização por escrito da gerência. A solicitação de autorização e da sua emissão deve prever que todos os passos sejam auditáveis.

Durante operação de emergência ou crise, o pessoal de suporte pode ser obrigado a remover, alterar ou inspecionar arquivos e mensagens pessoais sem autorização por escrito da gerência, para garantir que ataques sejam identificados e ações sejam tomadas para contê-los o mais brevemente possível. O pessoal de suporte deve consultar verbalmente a gerência sobre as medidas a serem tomadas, desde que isto não coloque em risco a segurança do sistema. Assim que a situação voltar ao nível de rotina, a gerência deve ser notificada por escrito e os procedimentos adotados neste nível de operação devem ser acionados.

As informações armazenadas ou em processamento no sistema, mensagens eletrônicas. o *Log* de Segurança e informações de monitoração poderão ser entregues às autoridades competentes para utilização como provas legais sempre que for julgado necessário pelo CESAR ou requisitado pelas autoridades.

Política de Integridade dos Recursos

A integridade dos recursos, serviços e informações do sistema é mantida através do cumprimento de todas as regras da Política de Segurança. No entanto, acidentes e

incidentes podem acontecer, colocando em risco a integridade dos recursos. Uma forma de recuperação da integridade do sistema após uma falha, vírus, uma operação não desejada ou após intrusões é através de replicação do recurso ou cópias de segurança *(backups).* Vírus e outros tipos de ataques por programas de computador também podem colocar em risco a integridade do sistema.

É responsabilidade dos administradores de sistemas implantar e atualizar programas anti-vírus e mantê-los funcionando automaticamente em todos os computadores da rede.

Todos os usuários são responsáveis por manter os programas anti-vírus ativos e atualizados na sua estação de trabalho e utilizá-los sempre que informações externas forem inseridas no sistema, via rede ou qualquer outro meio.

Qualquer impossibilidade de manter o anti-vírus funcionando deve ser comunicado à administração de sistemas em ocorrência por escrito (e-mail).

A integridade das informações armazenadas e em processamento no sistema deve estar garantida através da definição e implantação de procedimentos de replicação e de cópias de segurança que atendam aos seguintes requisitos:

- os recursos críticos devem estar disponíveis ininterruptamente;
- após uma falha de integridade, a recuperação da informação deve garantir a consistência, integridade e confiabilidade das informações recuperadas. Assim o sistema como um todo pode voltar a um estado seguro e consistente;
- os procedimentos de replicação ou *backup* devem ser completos, no sentido de preservar a integridade de todas os recursos, informações e serviços necessários à empresa e seus funcionários.

Os processos para realização de cópias de segurança e sua recuperação são descritos no Procedimento de *backup* definido pela administração de sistemas. Este procedimento define os seguintes aspectos:

- Freqüência e níveis de *backup*, horários de realização de *backup;*
- Tempo máximo aceitável para recuperação de informações a partir do *backup*, após a ocorrência de uma falha;
- Equipe responsável pela a realização do *backup* e recuperação de informações;
- Forma de solicitação de recuperação, com as autorizações necessárias.

A recuperação de informações privilegiadas deve ser autorizada por uma gerência, por escrito, e deve integrar o *Log* de Segurança do Sistema.

As cópias de segurança não devem ocupar o mesmo espaço físico que os servidores de onde as cópias são feitas.

Arquivos pessoais de usuários salvos em disco local são de inteira responsabilidade dos mesmos, inclusive para backup e confidencialidade da informação.

Política de Disponibilidade dos Recursos

Recursos e serviços de nível crítico devem estar disponíveis ininterruptamente durante operação de rotina do sistema. A não disponibilidade de um recurso ou serviço crítico é justificada somente quando a sua disponibilidade colocar em risco a segurança do sistema, nos casos de operá-lo em nível de emergência ou crise

A disponibilidade dos recursos e serviços não críticos está sujeita a regras definidas caso a caso para cada serviço.

Existe suporte 24 horas para os serviços críticos.

O suporte aos serviços não críticos é definido caso a caso para cada serviço.

A requisição de suporte segue procedimentos estabelecidos especificamente para este fim.
Os serviços de nível critico têm prioridade de suporte.

Solicitação de disponibilização de novos recursos computacionais, deve ser feita por escrito para o pessoal de suporte e será analisada caso a caso.

O pessoal do suporte deve manter constante atualização de versões e módulos de correção de bugs disponíveis para softwares críticos do sistema, que possam viabilizar a violação do sistema ou a indisponibilidade dos recursos computacionais.

Arquivos de usuários de interesse do CESAR devem ser disponibilizados na rede, para estarem passíveis dos procedimentos de proteção e backup e não devem ser salvos em discos locais.

Responsabilidades em Relação à Política de Segurança

É responsabilidade de todos os diretores, gerentes e funcionários da empresa cumprir e fazer cumprir as regras da Política de Segurança de acordo com o Termo de Compromisso previamente estabelecido e assinado pelos mesmos (em anexo, segue um modelo de Termo de Compromisso).

Dos Usuários

É esperado que todos os usuários possuam uma conduta consistente com as políticas aqui definidas. A violação das políticas acarretará ações disciplinares e/ou judiciais.

Abusos a outras redes de computadores através da rede da empresa, serão tratados como quebra das regras da Política de Segurança do CESAR.

Dos administradores de Sistema

As regras da Política de Segurança se aplicam aos administradores de sistema que, mesmo tendo privilégios de acesso, não podem utilizá-lo para contrariar as regras da Política de Segurança, salvo nos casos, em que, durante, a operação do sistema nos níveis de emergência ou crise, certas ações forem necessárias para manter a segurança do sistema.

Comunicação de Violação de Segurança

Qualquer violação das regras da Política de Segurança ou a realização de ações que possam colocar em risco usuários ou recursos do sistema computacional devem ser comunicados ao setor responsável.

A não comunicação de violações da política ou de atos que possam colocar em risco a segurança de usuários ou recursos do sistema computacional, constitui, em si, uma violação da Política de Segurança.

Comunicação de Problemas de Segurança

A não comunicação dos problemas encontrados nos software, aplicativos, ou sistemas corporativos que, possam colocar em risco a segurança de usuários ou recursos do sistema computacional, constitui, em si, uma violação da Política de Segurança.

Gerência da Política de Segurança

Log de Segurança do Sistema: o pessoal do suporte deve manter um *Log* de segurança do sistema com todas as informações pertinentes à Política de Segurança, monitorações do sistema, auditorias, etc.

Divulgação da Política de Segurança: o pessoal do suporte deve garantir que a Política de Segurança seja divulgada entre todos os funcionários, gerentes e diretores da empresa. Todos os usuários devem assinar um Termo de Compromisso, onde atestam que concordaram e aceitam os termos da Política de Segurança. Estes Termos de Compromisso devem integrar o *Log* de Segurança do sistema.

Mecanismos para garantir o cumprimento da política: é responsabilidade do CESAR a implantação de procedimentos (automatizados ou não) que garantam o cumprimento da Política de Segurança.

Exceções ao cumprimento das regras da Política de Segurança devem ser tratadas pelo pessoal de suporte. A autorização para o não cumprimento das regras da política deve ser emitida por escrito (e-mail) e passar a integrar o *Iog* de segurança do sistema.

A constante revisão da Política de Segurança é necessária para fazer frente aos avanços da tecnologia e surgimento de novos serviços, com suas conseqüências sobre a segurança dos sistemas computacionais. O pessoal do suporte deve coordenar o processo periódico de revisão da Política de Segurança e sua divulgação aos usuários.

Documentação e Treinamento para o Usuário

Os usuários constituem o elo mais fraco do sistema de segurança de um ambiente computacional pois possuem acesso interno e, algumas vezes, privilegiado aos recursos do sistema. Desta forma, erros não intencionais ou atuações maliciosas e criminosas por parte destes usuários são as mais difíceis de se detectar, pelo menos em tempo hábil para evitar danos. Além disto, uma vez que o acesso é autorizado, o dano causado por um usuário interno pode ser muito maior do que o de um invasor externo.

O treinamento adequado e o acesso à documentação sobre procedimentos e ferramentas que aumentem a segurança interna do sistema e da sua utilização são fatores fundamentais para que a Política de Segurança seja implantada com sucesso.

É permitido a intervenção por parte dos usuários para sugestões a respeito da Política de Segurança vigente. Inclusive a verificação, respeitando-se as normas, do cumprimento dessa política.

Referências:

[1] Apostila de Tópicos Avançados em Administração de Sistemas com conteúdo das aulas ministradas por Evandro Curvelo Hora.

[2] CANE. *User's Guide*. ImageNet Ltd: October 1997.

[3] Centro de Estudos e Sistemas Avançados do Recife. **http://www.cesar.org.br**. Disponível na Internet. 30 de Setembro de 1998.

[4] Proposta de Políticas de Segurança para Rede CESAR, Elionildo da Silva Menezes e Pedro Luciano Leite Silva, setembro de 1998

[5] RFC 1244

Pendências

Apêndice com RFC 1244
Termo de Compromisso – usuários do sistema
Apêndice c/Firewall