Secretaria de Defesa Social
Policia Militar de Pernambuco
Diretoria de Apoio Logístico
Centro de Processamento de Dados

Política de segurança da Rede QCG

QCG – Quartel do Comando Geral
Nilson Duarte Barbosa - Capitão PM

ÍNDICE

-Política de utilização de senhas
-Política de privacidade da informação

11 - POLÍTICA DE INTEGRIDADE DOS RECURSOS

12 - POLÍTICA DE DISPONIBILIDADE DOS RECURSOS

13 - RESPONSABILIDADE EM RELAÇÃO DA POLÍTICA DE SEGURANÇA

-Do Comando da PMPE
-Dos administradores de sistema
-Dos usuários

14 - COMUNICAÇÃO DE VIOLAÇÃO DE SEGURANÇA

15 - DOCUMENTAÇÃO E TREINAMENTO DOS USUÁRIOS

PREFÁCIO

A Política de segurança é uma ferramenta importante para definir normas e procedimentos de utilização dos ativos de uma determinada empresa visando à segurança de softwares e hardwares, devendo esta ser aplicada em todos os segmentos da empresa sem restrições.

1 - INTRODUÇÃO

O objetivo desse documento é desenvolver uma Política de Segurança para a rede do Quartel do Comando Geral podendo ser expandida para as demais OMEs da corporação, respeitando suas particularidades.

Segurança da Informação consiste na preservação da confidencialidade, integridade e disponibilidade da informação

.

A Política de Segurança está em conformidade as Portarias do Comando Geral, regulamentos e Leis existentes, e se preocupa com possibilidades de invasões externas, problemas de segurança local no sentido mais global.

Segundo Thomas A. Wadlow, “ A segurança deverá ser proporcional ao valor do que se está protegendo”. Ou seja, a implantação do sistema de segurança da informação tem de apresentar um custo benefício que torne a tentativa de ataque tão cara que desestimule o atacante, ao mesmo tempo em que ela é mais barata do que o valor da informação protegida.

QUEM FAZ A POLÍTICA?

A criação da política deve ser um esforço associado do pessoal técnico do CPD e dos Chefes e Diretores, que tem poder de fazer cumprir a política.

QUEM SÃO OS ENVOLVIDOS?

A política de segurança para ser efetivada deve ter aceitação do suporte e de todos usuários do Quartel do Derby, em especial os chefes de seções que apóiem a implementação do processo e que possam fazer cumprir as orientações da política.

RESPONSABILIDADES

O elemento chave para a implementação da política é que todos os envolvidos tenham a consciência de suas responsabilidades para a segurança e manutenção dos sistemas.

PENALIDADES

Consistem em punições administrativas para enquadramento daqueles que violarem as normas decorrentes desta Política de Segurança da Informação, visando incentivar a obtenção e manutenção do nível de segurança necessário ao trato das informações.

Deverão ser pré-definidas pela Diretoria, com apoio da Assessoria Jurídica, atendendo níveis diversos de
profundidade, para enquadramento de acordo com a gravidade e reincidência da violação da Política de Segurança.

As infrações ocorridas deverão ser analisadas pelo Gestor imediato do infrator
em conjunto com a Diretoria e com o Comitê Gestor de Segurança, que juntos, decidirão a aplicação ou não de punição e seu nível de enquadramento. Uma vez decidida pela aplicação da punição, esta, deverá ocorrer através de registro em ficha funcional e comunicação formal ao infrator.

COMUNICAÇÃO DA POLÍTICA DA SEGURANÇA

A política para se tornar efetiva deve ser publicada em Boletim Geral ou em Suplemento Normativo para que todos tenham ciência de suas responsabilidades, bem como é importante a realização de um forte treinamento com os usuários e administradores medidas essas fundamentais para o funcionamento e aceitação da política de segurança.

EDUCAÇÃO DO USUÁRIO

O usuário deve ser alertado de como o sistema computacional deve ser usado e como protegê-lo de usuários não autorizados, Sabe-se que grande parte dos problemas de segurança são originados na rede interna da organização e, muitas vezes, são causados pelo desconhecimento de conceitos e procedimentos básicos de segurança por parte dos usuários.Um exemplo clássico deste problema é a má configuração do programa de leitura de *emails* de um usuário, que faz com que qualquer arquivo anexado a uma mensagem seja automaticamente aberto ou executado, permitindo a instalação de *backdoors*, cavalos de tróia, disseminação de vírus na rede.

COOPERAÇÃO ENTRE ÓRGÃOS DO ESTADO

Contatos apropriados com as autoridades da A.T.I (Agência de Tecnologia da Informação), SDS (Secretaria de Defesa Social), CTIC (Centro de Tecnologia de Informação e Comunicações do Corpo de Bombeiro de PE, Unidade de Tecnologia da Informação da Polícia Civil) entre outros órgãos, devem ser mantidas para cooperação mútua, aconselhamento em casos de eventualidades similares e intercâmbio de informação sobre segurança em sistemas de informação.

ANÁLISE DE RISCO

A analise de risco serve para estimar o potencial de perdas associado às vulnerabilidades do sistema e quantificar o prejuízo que pode ocorrer, caso as ameaças se concretizem.

A analise de risco deve determinar

- O que deve ser protegido
- O que é necessário para garantir proteção

- Como proteger

Para isso a analise segue em duas fases

- Identificação dos bens
- Identificação das ameaças

Identificação dos bens e inventário

Consiste em ter um inventário de todas as coisas a serem protegidas pela política de segurança, passo importante para administração onde ela precisa ser capaz de ter o controle dos seus bens com seus valores relativos e suas identificações.

Os bens estão agrupados em:

-*Hardware* – O QCG possui um parque de 300 maquinas interligadas através de 25 (vinte e cinco) switchs, alguns gerenciáveis outros não e controlados por 5 (cinco) servidores um roteador e dois transciver conversores de fibra ótica.

-*Software* – Programas objetos, programas utilitários, sistemas operacionais, na relação se encontram o SIGRH (Web e stand alone), SISARM, WEBMAIL, SQL SERVER, WINDOWS XP, 2000, 2000 SERVER, 2003 SERVER, LINUX etc.

Identificação de ameaças

Consiste em identificar as ameaças para se tentar proteger os ativos da empresa.

- **Acesso não autorizado** – um acesso não autorizado seria o uso de uma conta de um outro usuário para ganhar acesso aos sistemas, ou a outros sistemas computacionais localmente.
- **Acesso autorizado, mas de má fé** – ocorre quando um usuário tem acesso permitido mas executa procedimentos de má fé. Podendo prejudicar a instituição ou conseguindo ganhos pessoais com as informações adquiridas.
- **Acesso através de códigos maliciosos** – ocorre quando códigos maliciosos inseridos em certos sites tomam o controle da máquina através de browsers, conseguindo informações das sua vitimas.

Disponibilização não autorizada de informações

1. voluntária – ocorre quando há um roubo proposital

2. involuntária – impressão de documentos sigilosos em impressoras publica ou em rede sem a devida manipulação do mesmo.

2 - POLÍTICA DE SEGURANÇA

ESCOPO

Esta política se aplica a toda rede do quartel do Derby, incluindo os servidores, estações de trabalho (desktops e notbooks) que estejam conectados a rede através de cabo tipo par "*transado categoria 5*" ou pela rede wireless (ainda em fase de implantação).

3 - 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 da rede do QCG.

- 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.

4 - NÍVEIS DE CONFIDENCIALIDADE DA INFORMAÇÃO

- Pública: informações que podem ser livremente acessadas por qualquer usuário exemplo: site da PMPE (www.pm.pe.gov.br).

- Privada: informações que podem ser acessadas por qualquer usuário interno devidamente cadastrado exemplo: SIGRH

  – Confidencial: informações que podem ser acessadas somente por usuário de um grupo restrito exemplo: LEV PM, Sistemas de controle de Armas.

5 - NÍVEIS DE CRITICIDADE DOS RECURSOS

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

- Windows Server
- Serviço de DNS
- Web Mail corporativo
- Firewall
- Banco de dados SQL Server
- Softwares próprios (Sigrh, Lev PM entre outros)
- Backups

6 - POLÍTICA DE ACESSO AOS RECURSOS E SERVIÇOS

Acesso físico aos recursos e segurança dos equipamentos

Deve existir uma área de recepção com atendentes ou outros meios de controlar o acesso físico a sala dos servidores, visitantes devem ser identificados e conduzidos a presença de algum administrador do sistema.

Nenhum equipamento ou software deve sair do QCG sem autorização. Os equipamentos particulares devem ser registrados na entrada. As pessoas devem ser conscientizadas de tais verificações ocorrerão.

O cabeamento de rede do sistema deve ser protegido e seu acesso deve ser permitido somente em pontos sob controle da administração de sistemas do Centro de Processamento de Dados (CPD). É proibido ligar computadores, equipamentos de rede e analisadores de tráfego não autorizados pelos administradores de rede.

O acesso à sala dos servidores deve ser acompanhado por um administrador de rede.

Os controles devem ser implementados para minimizar o risco de ameaças potenciais como: roubo, incêndio, fumaça, água, poeira, vibração, efeitos magnéticos, efeitos químicos.

Deve se levar em conta que devem ser proibidos lanches, bebidas e cigarros próximos aos equipamentos de processamento de informação.

Os equipamentos devem ser protegidos de falhas elétricas ou outras anomalias na eletricidade, as opções para a continuidade do fornecimento de

eletricidade incluem: múltiplas alimentações pra evitar um único ponto de falha no fornecimento de energia, aquisição de no-break, gerador sobressalente.

ACESSO LÓGICO: CONTAS DOS USUÁRIOS

Considerações gerais

Somente os Policiais lotados no QCG podem ter conta de login na rede. Existem duas categorias:

- Administradores de rede – possuem permissão para todos os diretórios;
- Usuários – Possuem diretórios com acesso individual.

Criação de contas

Existe uma única forma de criação de contas, definida em procedimento próprio, cada setor que necessite que um funcionário (PM ou Civil) tenha uma conta o chefe do setor deverá solicitar por escrito para que possa ser arquivada a referida documentação.

Ao criar a conta, o administrador de sistema deverá ter uma senha inicial que será alterada após o primeiro login na rede, é proibido criação de conta sem senha inicial.

Deverá ser entregue um documento para o usuário informando seus direitos e obrigações e o modo de usar sua conta de rede bem como os dias e horários que o mesmo poderá acessar a rede.

Gerenciamento de contas

Deve existir uma monitoração constante da utilização das contas dos usuários onde deve ser observada data, hora e local de utilização da conta, tentativa de acesso a pastas não autorizadas, tentativas de acesso a sites que estejam no elenco de sites impróprios (pedofilia, pornografia, etc.).

Contas inativas por um período de três meses serão bloqueadas.

Remoção de contas

Ao ser transferido para outra Unidade (capital ou interior) o usuário ou seu chefe deverá informar ao administrador de rede de sua transferência para que a conta possa ser removida.

Contas inativas por um período de seis meses serão removidas, e seus arquivos serão mantidos por um período de um ano.

Reabilitação de contas

A reabilitação das contas seguirão os mesmos tramites para a criação de contas, seus arquivos serão restabelecidos e disponibilizados para o usuário.

7 - UTILIZAÇÃO APROPRIADA DE RECURSOS

Os usuários podem usar somente sua conta pessoal, fica proibido a tentativa de mudar as restrições associadas a sua conta.
Os usuários são responsáveis pela utilização de software e outros materiais em meios eletrônicos de acordo com as Leis de copyright. É proibida a utilização de software pirata, instalação de jogos, envio de mensagens indecorosas, envio de material obsceno.

Acesso remoto

É proibida a existência e/ou utilização de acesso remoto (acesso a internet), por modem ou outro meio que não seja pelo link oferecido pelo CPD.

8 - ACESSO À INFORMAÇÃO CONFIDENCIAL

As informações confidenciais devem ser protegidas ao máximo. Quando armazenadas na rede deve existir um controle de permissões e mecanismo de criptografia que assegure sua confidencialidade.

Ao enviar informação confidencial pelo correio eletrônico o usuário deve:

1 – Criptografá-la ou utilizar qualquer outro mecanismo que torne a informação segura;

2 – Verificar os destinatários para ter certeza de que são autorizados a receber as informações;

3 – Verificar os membros das listas eletrônicas que são destinatárias da mensagem para ter certeza de que todos são autorizadas a receber as informações.

9 - 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 Server.

A segurança através de sistemas baseados em senha 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 devem ser mantidas e definidas, a política de senha inicial e política de uso de senhas.

Política de senhas iniciais

Ao abrir uma conta deve-se informar pessoalmente ao usuário a senha inicial. É de responsabilidade do administrador de segurança informar e explicar seu uso. Ao obter a senha o usuário receberá uma documentação explicando suas regras de utilização.

Política de uso de senhas

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

Os usuários devem trocar suas senhas a cada noventa dias. Elas não podem se repetir e não devem ser iguais as últimas seis anteriores. Após cinco tentativas a conta é bloqueada, sua reativação será feita mediante documentação e tal documento deve ser arquivado.

Política de privacidade da informação

Apesar de respeitar a privacidade dos usuários do sistema, os administradores têm o direito de auditar e monitorar processos do sistema, tentativas de acesso aos recursos de rede e do sistema computacional, utilização de tempo de CPU, acesso a arquivos etc.

Apenas em situação de suspeita, emergência ou algo de errado que possa estar acontecendo com o sistema, os administradores de sistemas do QCG, podem inspecionar o conteúdo das mensagens e arquivos, inclusive podendo arquivá-los ou removê-los caso seja necessário para manter o funcionamento do sistema.

As informações armazenadas ou em processamento no sistema, mensagens eletrônicas. O log de segurança e informações de monitoração poderá ser entregue as autoridades competentes para utilização como provas legais sempre que for julgado necessário ou requisitado por quem de direito.

10 - POLÍTICA DE DISPONIBILIDADE 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 é através de backups.

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

Todo o usuário é responsável por manter os programas antivírus ativos e atualizados na sua estação de trabalho e utilizá-los sempre que informação externa forem inseridas no sistema.

Qualquer impossibilidade de manter o antivírus funcionando deve ser comunicado à administração de sistemas em ocorrência por escrito ou por e-mail(suporte@pm.pe.gov.br).

A integridade das informações armazenadas e o processamento do sistema devem estar garantidas através de definição 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.

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 informação a partir do backup, após a ocorrência de uma falha;
- Equipe responsável pela realização do backup e recuperação de informações
- Forma de solicitação de recuperação, com as autoridades necessárias.

A recuperação de informações privilegiadas deve ser autorizada pelo Chefe do CPD, e deve integrar o log de segurança do sistema.

11 – 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 critico 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.

Os serviços de nível crítico têm prioridade de suporte, o pessoal de suporte deve manter constante atualização de versões e módulos de correção de bugs disponíveis para software críticos do sistema, que possam viabilizar a violação do sistema ou indisponibilidade dos recursos computacionais.

12 – RESPONSABILIDADE EM RELAÇÃO DA POLITICA DE SEGURANÇA

É responsabilidade de todos os chefes e diretores e demais policiais da PMPE que fazem uso da rede e dos sistemas cumprir as regras da Política de Segurança e cumprir

as atribuições e assumir responsabilidades específicas, com relação à Segurança

da Informação, segundo as suas competências.

.

Do Comando da PMPE

a. Aprovar a Política de Segurança;

b. Publicar Instrução Normativa implantando a Política de Segurança, definindo os prazos e procedimentos para adequação à mesma, bem como, as penalidades e procedimentos em caso de descumprimento da Política;

c. Disponibilizar os recursos necessários à implantação da Política de

Segurança;

d. Executar e fazer executar a Política de Segurança.

Dos Administradores de Sistemas e Redes e segurança

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

Tomar as providências de emergência, pertinentes à equipe de suporte, conforme plano de ação de resposta a incidentes sob responsabilidade da Equipe de Segurança da Informação e Redes.

Dos usuários

a. Cumprir as normas definidas na Política de Segurança;

b. Reportar, de imediato, ao CPD, qualquer incidente de segurança ou, até mesmo, suspeitas iminentes;

c. Sugerir medidas que possam elevar os níveis de segurança das instalações na sua área de atuação;

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

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

13 – COMUNICAÇÃO DE VIOLAÇÃO DE SEGURANÇA

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

A não comunicação de violação da Política de Segurança 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, bem como a não comunicação dos problemas encontrados nos software, aplicativos ou sistemas corporativos.

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, monitoração do sistema, auditorias, etc.

Divulgação da Política de Segurança: o pessoal de suporte de garantir que a Política de Segurança seja divulgada entre todos que trabalham no QCG, a divulgação deve ser continua ou seja: quando um policial ou funcionário chegar transferido para o QCG este deverá receber uma cópia da Política de Segurança e demais direitos e deveres de acesso a rede.

É muito importante que todos envolvidos com a segurança da informação tenham não só acesso ao documento, como também seja instruído no processo de implantação e uso da política, tendo conhecimento e formação adequada a eficácia do plano de segurança terá mais chance de sucesso. Além disso, todos passam ser co-responsáveis pelo processo uma vez que não podem alegar desconhecimento do mesmo.

Conforme explicado anteriormente, os aspectos de segurança física, lógica e

de pessoal, serão tratados em documentos independentes, tendo em vista suas peculiaridades e deverão compor este documento principal da Política de Segurança da Informação em forma de anexos, a fim de complementar com maior especificidade e detalhamento, as normas e recomendações de segurança no trato das informações, essas normas serão publicadas através de Portarias do comando Geral da Corporação.

Abaixo, segue a relação das demais Normas de segurança que serão trabalhadas com maior especificidade compondo os anexos acima referidos:

a) Normas de Segurança Física;

b) Normas de Segurança dos servidores;

c) Normas de Segurança de Aplicações;

d) Normas de Segurança para uso da Internet e do Correio Eletrônico;

e) Normas de Segurança de Rede;

f) Normas de Segurança para uso de Dispositivos Móveis;

g) Normas de Segurança para uso de Redes sem Fio;

h) Normas de Segurança para o Controle de Acesso (Autenticação);

i) Normas de Gestão de Tratamento de Vulnerabilidades Técnicas;

j) Normas de Gestão de Risco;

k) Normas de Gestão de Incidentes de Segurança;

l) Normas de Segurança para o Trato dos Equipamentos;

m) Normas de Segurança dos Sistemas de Informação;

n) Normas de Segurança de Recursos Humanos;

14 – DOCUMENTAÇÃO E TREINAMENTO DOS USUÁRIOS

Os usuários constituem o elo mais fraco do sistema de segurança de um ambiente computacional, pois possuem acesso interno e, algumas vezes, privilégios no sistema. Desta forma, erros não intencionais ou atuações maliciosas e criminosas por parte destes usuários são mais difíceis de detectar, pelo menos em tempo hábil para evitar danos. Além disto, uma vez que os acesos são autorizados, os danos causados por um usuário interno podem ser muito maior que um invasor externo.

O treinamento pode ser feito através de seminários programados, distribuições de cartilhas com informação, e-mails regulares com dicas sobre o assunto e site de divulgação.

Recife 28 de maio de 2009