Governo do Estado de **São Paulo**

Manual de Segurança em Ambientes Web

poupatempo

imprensaoficial

PRODESP Tecnologia da Informação

CASA CIVIL

GOVERNO DO ESTADO DE SÃO PAULO
RESPEITO POR VOCÊ

FOLHA DE CONTROLE DE REVISÕES

Número da versão	Data de emissão	Registro de modificações
00	23/08/2005	Versão Inicial
01		
02		
03		
04		
05		
06		
07		
08		
09		
10		

Sumário

Manual de Segurança em Ambientes Web

Recomendações de segurança para serviços eletrônicos do
Governo do Estado de São Paulo

1 Considerações Iniciais

A informação representa um dos bens mais valiosos de uma organização, garantindo a continuidade dos negócios, minimizando os riscos de perdas financeiras e a imagem da empresa no mercado. Em muitos segmentos a informação possibilita novas oportunidades de negócio e agiliza os atendimentos aos clientes de uma organização.

Pelo grau de importância que representa, a informação precisa ser adequadamente protegida. Para tanto, é preciso primeiramente levar em consideração as inúmeras formas nas quais a informação pode ser apresentada, como por exemplo, em papel, mídia eletrônica, e até mesmo falada. Além disso, a informação pode ser transmitida pelos mais variados meios, como e-mails, documentos, arquivos, apresentações e até mesmo em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, deve-se sempre protegê-la adequadamente.

A segurança da informação é baseada em três pilares: confidencialidade (garantia de que a informação é acessível somente por pessoas autorizadas), integridade (salvaguarda da exatidão e completude da informação) e disponibilidade (garantia de acesso à informação sempre que preciso).

A interconexão das diversas redes do governo com as redes públicas e privadas e o compartilhamento de recursos de informação, aumentam a dificuldade de se controlar o acesso e os riscos envolvidos, permitindo a ocorrência cada vez mais freqüente de fraudes eletrônicas, espionagem, sabotagem, vandalismo, problemas causados por vírus, *hackers* e ataques do tipo *denial of service* (indisponibilização dos serviços), entre outros.

A gestão da segurança da informação necessita do apoio e participação de todos os funcionários efetivos e terceirizados. Pode ser necessário o envolvimento também de fornecedores, clientes e parceiros, além de consultorias externas especializadas.

Este manual tem como propósito prover uma base comum para as práticas efetivas de gestão da segurança e viabilizar a confiança nos relacionamentos entre as organizações (G2G - governo x governo, G2C - governo x cidadão, G2B - governo x empresas). Convém que as recomendações descritas neste documento sejam selecionadas e usadas de acordo com a legislação e as regulamentações vigentes.

É importante que o leitor tenha conhecimento da literatura aconselhada e use as recomendações deste documento de forma **complementar** a esta literatura.

A simples aplicação destas recomendações auxilia, porém não garante a segurança da informação. Um processo visando exclusivamente a segurança deve ser implementado desde o momento da concepção dos projetos, incluindo testes de análise de riscos para que as metas de segurança sejam de fato atingidas.

2 Segurança Física do Ambiente

2.1. Segurança Física

Os recursos e instalações de processamento de informações críticas ou sensíveis ao negócio devem ser mantidos em áreas seguras, protegidas por um perímetro de segurança definido, com barreiras de segurança apropriadas e controle de acesso.

A proteção física pode ser alcançada através da criação de diversas barreiras em torno da propriedade física do negócio e de suas instalações de processamento da informação. Cada barreira estabelece um perímetro de segurança, contribuindo para o aumento da proteção total fornecida. A proteção fornecida deve ser proporcional aos riscos identificados, sendo necessário a implementação de controles de entrada apropriados para assegurar que apenas pessoas autorizadas tenham acesso as informações.

As paredes externas do local devem ser sólidas e todas as portas externas protegidas de forma apropriada contra acessos não autorizados, como, por exemplo, mecanismos de controle, travas, alarmes, etc.

Deve-se levar em consideração as possibilidades de dano causado por fogo, inundação, explosão, manifestações civis e outras formas de desastres naturais ou causados pelo homem.

Ainda com relação aos aspectos citados, recomenda-se o seguinte:

a) Isolar as instalações críticas do acesso público, mantendo os servidores em local reservado com acesso controlado;
b) Manter um controle restrito de entrada e saída de pessoas no recinto, utilizando sistemas de controle de entrada através de códigos de acesso, crachás autorizados entre outras tecnologias disponíveis no mercado;
c) Jamais permitir a instalação de equipamentos que permitam a duplicação de informações no mesmo ambiente em que as mesmas se encontram ou dentro de áreas de segurança, como por exemplo, fotocopiadoras, scanners, unidades de gravação de CDs e máquinas de fax, para evitar vazamento de informação;
d) Proibir a entrada de filmadoras e câmeras fotográficas nestes ambientes;
e) Portas e janelas devem ser mantidas fechadas quando não utilizadas e, sempre que possível, implementar um sistema de alarme.

2.1 Segurança dos Equipamentos

Deve-se proteger os equipamentos (incluindo aqueles utilizados fora das instalações físicas da organização) de forma a reduzir o risco de acessos não autorizados aos dados mantidos nestes ambientes contra perda ou violação dos mesmos. Esta proteção deve considerar os equipamentos instalados e os em alienação.

Devem ser implementados controles especiais para proteção contra acessos não autorizados às instalações de infraestrutura que mantém o ambiente em operação, tais como as cabines de fornecimento de energia elétrica e salas que possuem equipamentos utilizados na distribuição dos cabeamentos lógicos. Além disso, convém que todo o cabeamento (elétrico, de telecomunicação e de rede) que viabilize a transmissão de dados e serviços relacionados à informação, seja protegido contra danos e interceptação. Recomenda-se, para tanto, a utilização de uma estrutura de cabeamento independente.

Deve-se prever para os equipamentos críticos ao negócio, uma proteção contra falhas de energia e outras anomalias na alimentação elétrica, utilizando sistemas de *no-break* que possam suprir uma eventual pane elétrica, ou até mesmo geradores de energia elétrica.

Além da manutenção permanente dos equipamentos de maneira a garantir a continuidade da disponibilidade e integridade dos processos críticos, deve-se manter recursos sobressalentes como contingência, para casos de falhas.

Equipamentos que realizam acessos remotos às instalações do órgão, também devem prever mecanismos de segurança equivalentes aos utilizados dentro da entidade que provê a informação. Dentre os equipamentos que se enquadram nesta categoria, estão as variações de computadores pessoais, como agendas eletrônicas, telefones móveis, *notebooks, Palms*, etc, os quais são utilizados em viagens, trabalhos domésticos ou serviços externos ao ambiente normal de trabalho.

Informações que deixaram de ser úteis à organização em determinado momento, devem ser destruídas para que não caiam em mãos estranhas e com isso possam trazer qualquer prejuízo a organização. Para tanto é preciso que se implemente formas eficazes de inutilização física das mesmas, impedindo assim sua reutilização.

Uma vez que o ambiente não conte com uma infra-estrutura adequada à segurança física dos equipamentos, recomenda-se a instalação dos mesmos no ambiente de Data Center do Estado.

3 Segurança Lógica

Deve-se manter os procedimentos de operação identificados pela política de segurança, documentados e atualizados. Convém que os procedimentos operacionais sejam tratados como documentos formais e que as mudanças sejam autorizadas pela direção da organização.

Deve-se documentar os procedimentos das atividades associadas com os recursos de comunicação e de processamento das informações, tais como procedimentos de ativação e desativação de servidores/estações, geração de cópias de segurança (*back-up*) e sua recuperação (*restore*), rotinas de manutenção de equipamentos, controle da segurança das informações, gestão do tratamento das correspondências e procedimentos relacionados às atividades executadas no CPD.

3.1. Política de Controle de Acesso

Deve-se definir e documentar os requisitos do negócio para controle de acesso a ambientes considerados restritos. As regras de controle de acesso e direitos para cada usuário ou grupo de usuários devem ser claramente estabelecidas no documento da Política de Controle de Acesso.

O estabelecimento de regras deve ser baseado na premissa "Tudo deve ser proibido a menos que expressamente permitido", ao invés da regra "Tudo é permitido a menos que expressamente proibido".

3.2. Controle de Acesso à Rede

Os acessos internos e externos aos serviços de rede devem ser controlados e liberados de acordo com a necessidade de cada usuário, dependendo do tipo de acesso, caminho utilizado, criticidade das informações, recursos a serem disponibilizados, entre outros.

Os pontos de rede devem ser protegidos (com autenticação, por exemplo) para impedir a conexão de estações não autorizadas.

O acesso às portas de diagnóstico dos equipamentos (*switches, routers*, etc.) deve ser seguramente controlado.

É preciso segmentar as redes logicamente, isolando os servidores de missão crítica ou sensíveis ao negócio da organização (uma rede para os servidores e outra para as estações), cada uma das quais protegidas por um perímetro de segurança definido. Tal perímetro pode ser implementado com a instalação de um *gateway* seguro entre as duas redes que serão interligadas para controlar o acesso e o fluxo de informações entre os dois domínios. Este *gateway* deve ser configurado para filtrar o tráfego entre estes dois domínios bloqueando acessos não autorizados de acordo com a política de controle de acesso da organização. Um exemplo deste tipo de *gateway* é freqüentemente referenciado como *firewall*.

As funcionalidades de segurança do sistema operacional, quando existentes, devem ser usadas para restringir o acesso aos recursos computacionais. Além disso, convém que os acessos aos serviços de informação sejam realizados através de um processo seguro de entrada no sistema (*log-on*).

Terminais inativos em locais de alto risco, por exemplo, em áreas públicas ou externas (fora dos limites do gerenciamento de segurança da organização), ou servindo a sistemas de alto risco, devem contar com sistema de desligamento automático após um período predeterminado de inatividade, de forma a prevenir contra o acesso de pessoas não autorizadas.

A mesma preocupação deve ser necessária com relação à computação móvel (*notebooks*, *palmtops, laptops*, telefones celulares, etc) e acessos remotos, adotando-se, por exemplo, recursos de autenticação forte e criptografia.

3.3. Gerenciamento das Informações

O gerenciamento da segurança de redes que se estendam além dos limites físicos da organização, requer particular atenção. Além disso, também pode ser necessário a utilização de controles adicionais para proteção de dados sensíveis que transitam por redes públicas.

É imprescindível a utilização de um conjunto de controles, de forma a obter e preservar a segurança nas redes de computadores. Para tanto, devem ser implementados controles para garantir a segurança de dados nas redes, assim como a proteção dos serviços disponibilizados contra acessos não autorizados.

3.3.1. Segurança e Tratamento das Informações

Deve-se definir uma política de geração de cópias de segurança das informações de vital importância para a organização armazenadas nos servidores utilizando mídias digitais (óticas e/ou magnéticas).

As mídias devem ser controladas e fisicamente protegidas, sendo armazenadas em locais seguros contra roubo, furto e incêndio, utilizando, por exemplo, cofres especialmente projetados para esta finalidade.

Os Data Centers podem ser utilizados também para espelhamento dos ambientes existentes na organização, mantendo desta maneira os serviços prestados ao cidadão disponível, mesmo na ocorrência de qualquer eventualidade. De forma semelhante, os Data Centers podem espelhar serviços críticos entre si, aumentando o nível de segurança. Esta é uma boa alternativa para um plano de continuidade de negócios.

3.3.2. Integridade do Ambiente

Deve-se adotar uma política de atualização das correções de segurança dos sistemas operacionais utilizados em toda a organização, ou seja, analisar todas as vulnerabilidades encontradas e publicadas nos meios de comunicação e aplicar as devidas correções, tanto nos servidores quanto nas estações dos usuários.

A entidade da Administração Pública ou órgão deve dispor de ferramentas que combatem e impedem a disseminação dos mais diversos tipos de *malwares* (vírus, *worms* e outras pragas virtuais), como sistemas de anti-vírus e *anti-spywares*.

3.3.3. Segurança do Correio Eletrônico

Deve-se implementar controles para se reduzir os riscos gerados pelo uso do correio eletrônico nas organizações. Esses controles incluem:

a) Levantamento de possíveis vulnerabilidades das mensagens a acessos não autorizados, que permitam sua modificação ou negação do serviço;
b) Levantamento de possíveis vulnerabilidades a erros, como por exemplo, endereçamento e direcionamento incorretos;
c) Considerações legais relacionadas à necessidade potencial de prova de origem, envio, entrega e aceitação;
d) Divulgação externa de listas de funcionários;
e) Acessos dos usuários remotos às contas de correio eletrônico.

3.3.3.1. Política de Uso do Correio Eletrônico

Todo o sistema de correio eletrônico deverá definir uma política clara para a utilização do correio eletrônico, quanto a:

a) Ataques por vírus e interceptação da mensagem;
b) Proteção de anexos;
c) Orientações quanto ao uso adequado da solução;
d) Responsabilidades dos usuários, de forma a não comprometer a organização;
e) Uso de técnicas de criptografia para proteger a confidencialidade e integridade das mensagens eletrônicas;
f) Retenção de mensagens que, se guardadas, podem ser descobertas e utilizadas em casos de litígio;
g) Controles adicionais para a investigação de mensagens que não puderem ser autenticadas.

Uma vez que o ambiente não conte com uma infra-estrutura adequada à segurança lógica dos equipamentos utilizados para a disponibilização do serviço de Correio Eletrônico, recomenda-se a instalação do mesmo no ambiente de Data Center do Estado.

4 Hospedagem

Todos os órgãos e entidades da Administração Pública Estadual deverão utilizar obrigatoriamente os "*Data Centers*" implementados pelo Governo do Estado para hospedagem, publicação de informações e serviços eletrônicos prestados por meio da Internet.

Cada uma dessas entidades deve nomear um responsável técnico pela segurança de seus ambientes, com ao menos um suplente, para, além de definir e auditar as políticas de segurança de seu ambiente, receber notificações, orientações a atualizações de procedimentos de segurança provenientes da Administração Central de Segurança da Informação do ambiente a que está conectado. É importante salientar que estes profissionais, a serem nomeados pelos órgãos, devem estar em exercício nos órgãos ou entidades, não cabendo esta função à terceiros, já que estes profissionais poderão ter acesso às informações e procedimentos de segurança da organização.

A guarda e o manuseio das informações deverão obrigatoriamente estar sob a responsabilidade dos órgãos e entidades da Administração Pública Estadual.

Os ambientes de Data Center do Estado contam com uma infra-estrutura apropriada para hospedagem de servidores e serviços (acesso restrito e controlado, *no-break*, gerador, recursos de climatização, segurança, monitoramento, gerenciamento, e facilidades para atualização remota das informações), permitindo sua publicação na Internet e na Intranet do Governo. Este serviço, que é oferecido às Secretarias, órgãos e entidades vinculadas ao Governo, visa garantir a confiabilidade e disponibilidade necessária ao seu negócio.

Com relação a hospedagem de servidores, estes ambientes oferecem duas modalidades: *Colocation* e *Hosting*.

4.1. Colocation

Esta modalidade de hospedagem prevê o acondicionamento dos servidores das Secretarias, Órgãos e entidades do Governo em um ambiente com acesso restrito, o qual conta com recursos de climatização, segurança, monitoramento 24 x 7, gerenciamento e atualização remota, permitindo também a publicação dos serviços na Internet e na Intranet do Estado.

Dentre as vantagens oferecidas para esta modalidade, estão:

a) Segurança no acesso das informações
b) Confiabilidade quanto a integridade das informações
c) Monitoramento contínuo dos equipamentos que mantém as informações
d) Facilidade de escalabilidade com redução de custos com instalações de servidores
e) *Backup* periódico dos dados

4.2. Hosting

Esta modalidade oferece equipamentos e instalações projetadas especificamente para hospedar o conteúdo, as aplicações e os serviços das Secretarias, Órgãos e entidades vinculadas ao Governo do Estado, de acordo com as necessidades exigidas pelo grau de importância desses sistemas, utilizando para isso, recursos exclusivos do Data Center do Governo. Dentre estes recursos estão: infra-estrutura elétrica e lógica, servidores de alta performance e disponibilidade, gerenciamento de conectividade, servidores e aplicações, entre outros.

Dentre as vantagens oferecidas para esta modalidade, estão:

a) Solução de hospedagem customizada de acordo com as necessidades do cliente
b) Segurança, controle, qualidade e flexibilidade na disponibilização das informações
c) Backup periódico dos dados
d) Proteção com antivírus atualizado diariamente
e) Aplicação regular de *patches* de atualização
f) Atualização tecnológica (*upgrades*) de hardware e software
g) Redução de custos com investimentos em infra-estrutura, software, equipamentos, contratos de manutenção, treinamento e manutenção de equipe de profissionais.

5 Monitoramento

5.1. Equipamentos

Para garantir a continuidade dos serviços, os recursos dos equipamentos devem ser constantemente monitorados, permitindo não só a identificação de possíveis problemas, mas também futuras atualizações de acordo com a tendência de crescimento de seus programas e aplicativos (*capacity-planning*). O monitoramento desses recursos deve verificar:

a) Espaço disponível em disco;
b) Processamento;
c) Utilização de memória;
d) Status do serviços;
e) Inventário de segurança (*patches*, correções, bibliotecas de antivírus, etc);
f) Conectividade.

Além desses, é recomendado monitorar os demais recursos fundamentais do ambiente, como por exemplo:

a) Sistema de alimentação elétrico;
b) Climatização (ar-condicionado, umidade);
c) *No-breaks* (carga e situação das baterias) e geradores;
d) Conectividade de rede (situação da rede local, *links*, *switches*, *hubs*, roteadores, etc.)

5.2. Serviços

Os sistemas devem ser monitorados para detectar divergências entre a política de controle de acesso e os registros de eventos monitorados, fornecendo evidências no caso de incidentes de segurança.

Trilhas de auditoria registrando as exceções e outros eventos de segurança relevantes, devem ser produzidas e mantidas por um período de tempo determinado pela área de Administração da Segurança da Informação da organização, pois estas auxiliarão à futuras investigações e na monitoração do controle de acesso. Os registros (*logs*) de auditoria devem incluir:

a) Identificação dos usuários;
b) Data e horário de entrada (*log-on*) e saída (*log-off*) no sistema;
c) Identidade do terminal e, quando possível, a sua localização;
d) Registros das tentativas de acesso ao sistema (aceitas e rejeitadas);
e) Registros das tentativas de acesso a outros recursos e dados (aceitas e rejeitadas).

Para uma correta leitura dos diversos *logs* espalhados pelo ambiente, visando facilitar eventuais investigações que se façam necessárias, convém que todos os horários dos servidores sejam sincronizados, utilizando-se, por exemplo, o UTC (*Universal Time Coordinated* ou Tempo Universal Coordenado) ou GPS (*Global Positioning System* ou Sistema de Posicionamento Global).

6 Modelo Organizacional

Um ponto importante na definição da estrutura de segurança é a definição e adoção de um Modelo Organizacional, levando em consideração a variedade de culturas, ambientes e recursos disponíveis na organização.

Todos os modelos são baseados na criação de um Grupo de Respostas à Incidentes, que pode seguir um dos modelos apresentados a seguir.

6.1 Interno Distribuído

É o modelo inicial para o gerenciamento correto de incidentes. Possui um Coordenador para responder aos incidentes em conjunto com as áreas envolvidas (necessárias para resolver o problema). Dessa forma, os profissionais responsáveis pela solução do incidente, sob a supervisão do coordenador do grupo, conseguem solucionar e manter o material necessário para se analisar o incidente.

O coordenador desse grupo não precisa ser uma pessoa especializada em Segurança da Informação, mas sim uma pessoa que se preocupe não somente em resolver o incidente, mas também em procurar as causas e trabalhar para que o mesmo evento não volte a ocorrer.

6.2 Interno Centralizado

Modelo onde os membros do grupo trabalham exclusivamente na área de Segurança, oferecendo serviços pró-ativos, reativos e de qualidade de serviço à organização, atuando também diretamente na resolução dos problemas e na manutenção das informações necessárias para investigação das causas e propostas de solução para mitigação dos impactos.

6.3 Combinado (Centralizado e Distribuído)

Modelo que utiliza recursos existentes dentro das áreas de suporte das organizações, adicionados a alguns recursos que trabalham exclusivamente na área de Segurança.

Dessa forma, os membros centralizados do time executam as atividades pró-ativas e de qualidade de serviço, enquanto os membros distribuídos atuam nas atividades reativas e em algumas atividades pró-ativas, porém como tarefas de sua atividade principal nas áreas de suporte.

6.4 Coordenador

Modelo que pode ser bastante funcional para entidades que possuem órgãos ligados diretamente, onde a entidade organiza um grupo que coordena os demais grupos de segurança dos órgãos. Dessa maneira, torna seu trabalho mais eficiente e as atividades padronizadas em todas as sucursais da entidade.

Outra forma de utilizar esse modelo é coordenando e auxiliando outros grupos que são "associados" a ele e que utilizam seus contatos e conhecimentos para o gerenciamento de seus incidentes. No Brasil, o CERT[1] tem esse papel, sendo muito útil como fonte de informação e contato com outros CSIRTs[2], tanto no Brasil quanto em outros países, uma vez que tem reconhecimento mundial.

Envolvimento do Grupo de Incidentes e Respostas de Segurança com áreas não técnicas da organização.

Normalmente os grupos de resposta a incidentes possuem interação muito forte ou fazem parte das equipes de tecnologia da empresa, entretanto é muito importante o seu relacionamento com outras áreas da empresa, como Recursos Humanos e Departamento Jurídico.

A interação com essas áreas da empresa pode ser muito útil na resolução e análise de incidentes, uma vez que podem ocorrer questões que envolvam o relacionamento com funcionários da empresa ou a necessidade de uma averiguação em contratos.

Terceirização do Grupo de Incidentes e Respostas de Segurança.

Devido a restrições orçamentárias ou de recursos profissionais, algumas organizações optam por terceirizar a atividade de Grupo de Incidentes e Respostas de Segurança ou parte dela. O principal ponto a favor dessa opção baseia-se no nível de especialização da empresa contratada que normalmente possui especialistas para cada serviço prestado.

Essa terceirização deve ser conduzida e analisada com muito cuidado, devido aos riscos associados à mesma, tais como:

a) Relação de confiança com a empresa contratada para a prestação do serviço;
b) Dependência da empresa em relação às tecnologias e processos;
c) Questões legais de acesso à informações, já que a empresa contratada terá acesso as informações que podem ser confidenciais.

[1] Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança do Brasil
[2] Grupo de Resposta a Incidentes de Segurança em Computadores

Escolha do modelo do Grupo de Incidentes e Resposta de Segurança.

Não existe uma receita para a escolha do modelo correto do grupo. O que é aconselhável é que, primeiramente, sejam verificadas algumas informações na organização, tais como:

a) Quais serviços e atividades serão prestados;
b) Quais recursos de pessoal, infra-estrutura, software e orçamento estarão disponíveis para a montagem do grupo;
c) Quais as expectativas da organização em relação ao trabalho do grupo.

Com os modelos citados acima é possível utilizar um dos cinco ou então fazer a combinação de modelos, tornando possível a implantação do Grupo de Incidentes e Respostas de Segurança que melhor se adapte à realidade da empresa.

7 *Outras Fontes de Pesquisa*

Comitê Gestor da Internet no Brasil: http://www.cg.org.br/

NIC BR *Security Office:* http://www.nbso.nic.br

CAIS-Centro de Atendimento a Incidentes de Segurança: http://www.rnp.br/cais/

Governador do Estado
Geraldo Alckmin

Secretário da Casa Civil
Arnaldo Madeira

Secretário de Estado de Comunicação
Roger Ferreira

Secretaria de Estado de Comunicação
Emerson Figueiredo
Patricia Ribas Reis Guedes

Sistema Estratégico de Informações
Roberto Meizi Agune

Prodesp
Paulo Sérgio Varella
Douglas Viudez

Imprensa Oficial
Hubert Alquéres
Fernando Henrique Guarnieri

Fundap
Neide Hahn

e-Poupatempo
Álvaro Gregório
Américo C. Santos Neto
Carlos Torres

Ficha Técnica

Redação e Edição
Marcos Tadeu Yazaki

Editoração Gráfica
Américo C. Santos Neto

Editoração Eletrônica
André Rodrigues

Agradecimentos
Wagner Moreno
Olyntho Meneguzzi Junior
Clovis Simabuku
Fabio Neves Fernandes

Este manual está disponível em versão eletrônica:
www.cqgp.sp.gov.br