



Título: Apresentação Foco Security – 13 Páginas

Palavras Chaves: Segurança da Informação, Análise de Risco, Plano de Continuidade, Teste de Invasão
São Paulo -SP

www.focosecurity.com.br

Sumário	Pág.
1. A Foco Security	03
2. Introdução à Segurança da Informação	04
3. Análise de Risco	06
4. Plano de Continuidade	09
5. Classificar Informação	09
6. Política de Segurança da Informação	10
7. Comitê Corporativo de Segurança da Informação	10
8. Teste de Invasão	10
9. Campanha de Divulgação	11
10. Avaliação de Segurança em Aplicações	11
11. Política de Segurança já Implantada	11
12. Gerenciamento e Manutenção da Sua Segurança	12
13. Monitoramento de Sites	12
14. Motivos para contratar a Foco Security	12
15. Conclusão	13
16. Contato Comercial	13
17. Informações sobre o Conteúdo deste documento	13

1. A Foco Security

A **Foco Security** oferece serviços na área de Segurança da Informação, com um grande diferencial, ter se desenvolvido em parceria com a **Empresa Júnior das Faculdades Tancredo Neves** (www.tancredo.br).

Utilizando este modelo de negócio, foi possível se concretizar no mercado, conquistar clientes e parceiros. Hoje em sua carteira de clientes destacam-se montadoras de veículos, seguradoras, locadoras de veículos, empresas de desenvolvimento de sistemas, Empresas de manufatura entre outras. A **Foco Security** desenvolve e implantando soluções em Segurança da Informação para pequenas, médias e grandes empresas.

*“67% das empresas brasileiras pretendem investir em
Segurança da Informação”*

Fonte: Agence Interativa

*“74% dos entrevistados detectaram incidentes de segurança,
sendo que 68% também reportaram incidentes de
proveniência **interna**.”*

Fonte: CSII/FBI 2003

*“O roubo de informação proprietária representa a
maior perda financeira.”*

Fonte: CSII/FBI 2003

*“82% detectaram infecções de seus sistemas por vírus de
computador.”*

Fonte: CSII/FBI 2003

*“O tráfego de **spams** vai dar um salto de **3 bilhões** de
mensagens por dia para **17,7 bilhões até 2008**.”*

Fonte: Ferris Research

2. Introdução à Segurança da Informação

A informação é um ativo que, como qualquer outro ativo importante para sua empresa, tem um valor e obviamente necessita ser adequadamente protegida. A segurança da informação protege a informação de diversas ameaças com o objetivo de garantir a continuidade dos negócios, minimizar os danos aos negócios, maximizar o retorno dos investimentos e as oportunidades de negócio.

A informação pode existir de diversas formas. Pode ser impressa, escrita, armazenada de forma eletrônica, transmitida via e-mail, mostrada em filmes ou falada em conversas. Independente da forma que é apresentada ou meio pelo qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida de forma adequada.

A segurança da informação visa preservar os seguintes itens:

a) Confidencialidade: Garantir de que a informação é disponibilizada apenas para pessoas autorizadas.

b) Integridade: Garantir que a informação esteja sempre na forma original que foi disponibilizada, em outras palavras, impedir que algum agente altere a informação sem autorização.

c) Disponibilidade: Garantir de que as pessoas autorizadas tenham acesso à informação e aos ativos sempre que necessário.

Segurança da informação é obtida a partir da implementação de diversos controles, que podem ser, políticas de segurança, procedimentos, controles via hardware e software, entre outros. Estes controles precisam ser estabelecidos para garantir que os requisitos de segurança da organização sejam atendidos.

A informação, processos da empresa, softwares, hardwares, sistemas e redes são importantes ativos. **Confidencialidade, integridade e disponibilidade** da informação são essenciais para preservar a competitividade, lucratividade, requisitos legais e a imagem da empresa perante seus clientes e parceiros.

Os sistemas de informação e redes de computadores são colocados à prova por diversas ameaças à segurança da informação que são originadas de diversas fontes: Fraude eletrônica, espionagem, sabotagem, vandalismo, fogo, inundação, funcionário insatisfeito, concorrentes entre outros. Problemas de segurança causados por vírus, hackers e ataques de denial of service (negação de serviço) estão se tornando cada vez mais comuns e mais perigosos para empresas.

A dependência nos sistemas de informação e serviços mostra que as organizações estão cada vez mais vulneráveis às ameaças de segurança. Conexões com diversas redes, públicas ou privadas e a necessidade do compartilhamento de informação aumentam a dificuldade o controle de acesso. A computação distribuída dificulta o desenvolvimento de procedimentos para um controle de acesso eficiente.

Diversos sistemas de informação não foram projetados para serem seguros. A segurança que pode ser desenvolvida por meios técnicos é limitada e convém que seja apoiada e completada por procedimentos e normas apropriados. Isto requer

um planejamento cuidadoso e com atenção aos detalhes. A gestão da segurança da informação precisa também da participação de todos os funcionários, parceiros e muitas vezes clientes e fornecedores da empresa. Consultoria externa especializada pode ser também necessária.

É essencial que uma organização identifique os seus **requisitos de segurança**.

Existem três fontes principais.

A **primeira fonte** é derivada da **análise de risco** dos ativos. A análise de risco identifica ameaças aos ativos, vulnerabilidades e probabilidade de ocorrência. O impacto e projeção de perda financeira também é estimado.

A **segunda fonte** é a legislação vigente, regulamentações e contratos que a empresa, parceiros, funcionários e prestadores de serviço tem que atender.

A **terceira fonte** é o conjunto de princípios e requisitos para o processamento da informação.

3. Análise de Risco

Os requisitos de segurança são identificados através de uma avaliação sistemática dos riscos de segurança. Os gastos com os controles necessitam ser balanceados de acordo com os danos causados aos negócios gerados pelas potenciais falhas de segurança. As técnicas de avaliação de risco podem ser aplicadas em toda a organização ou apenas em parte dela, assim como em um sistema de informação individual, componentes de um sistema específico ou serviços, quando for viável, prático e útil.

A avaliação de risco é uma consideração sistemática:

- a) do impacto nos negócios como resultado de uma falha de segurança, levando-se em conta as potenciais conseqüências de perda de confidencialidade, integridade ou disponibilidade da informação ou de outros ativos;
- b) da probabilidade de tal falha realmente ocorrer a luz das ameaças e vulnerabilidades mais freqüentes e nos controles atualmente implementados.

Os resultados dessa avaliação ajudarão a direcionar e determinar ações gerenciais e prioridades mais adequadas para um gerenciamento dos riscos de segurança da informação e a selecionar os controles a serem implementados para a proteção contra estes riscos. Pode ser necessário que o processo de avaliação de riscos e seleção de controles seja executado um determinado número de vezes para proteger as diferentes partes da organização ou sistemas de informação isolados.

É necessário realizar análise críticas periódicas dos riscos de segurança e dos controles implementados para:

- a) considerar as mudanças nos requisitos de negócio e suas prioridades;
- b) considerar novas ameaças e vulnerabilidades;
- c) confirmar que os controles permanecem eficientes e adequados

Convém que as análises críticas sejam executadas em diferentes níveis de profundidade, dependendo dos resultados das avaliações de risco feitas anteriormente e das mudanças nos níveis de riscos que a direção considera aceitável para os negócios. As avaliações de risco são sempre realizadas primeiro em nível mais geral, como uma forma de priorizar recursos em áreas de alto risco, e então em um nível detalhado, para solucionar riscos específicos.

Uma vez tendo sido identificados os requisitos de segurança, convém que os controles sejam selecionados e implementados para assegurar que os riscos são reduzidos a um nível aceitável. Os controles podem ser selecionados a partir desta Norma ou de outro conjunto de controles, ou novos controles podem ser desenvolvidos para atender às necessidades específicas, quando apropriado. Existem diversas maneiras de gerenciar os riscos.

Convém que os controles sejam selecionados baseados nos custos de implementação em relação aos riscos que serão reduzidos e as perdas potenciais se as falhas na segurança ocorrerem. Convém que fatores não financeiros, como, por exemplo, prejuízos na reputação da organização, sejam levados em consideração.

Uma forma de realizar a análise de risco é como disposto na **figura 1** abaixo

Ameaça	PA	Exploração	FC	E	Vulnerabilidade	FV	Ativo	PrA
Atacante	0,6	Ataque de Força Bruta	10	1	Falta de diretivas de senha	10	Contas de Administradores de Empresa	10
Código mal-intencionado	0,6	Code Red	9	3	Vulnerabilidades de ida/idaq	8	Servidores IIS de departamento	6
Código mal-intencionado	0,6	Code Red	9	3	Vulnerabilidades de ida/idaq	8	Servidores IIS de recursos humanos	7
Atacante	0,6	Ferramenta de enumeração de NetBIOS	6	2	sessões nulas	10	Controlador de domínio raiz	8
Incêndio	0,1	Curto Cicuito	9	1	Fiação elétrica não conforme com especificação mínima	6	Controlador de domínio raiz	8

FR	NFA	FI	FE	EPU	TOA	EPA
10	6	100	0,60	R\$ 497.400,00	0,5	R\$ 248.700,00
3	1,8	48	0,09	R\$ 35.000,00	0,35	R\$ 12.250,00
3	1,8	56	0,10	R\$ 22.000,00	0,7	R\$ 15.400,00
3	1,8	80	0,14	R\$ 789.500,00	0,2	R\$ 157.900,00
9	0,9	48	0,04	R\$ 789.500,00	0,01	R\$ 7.895,00

Figura 1 – Análise de Risco

Após a identificação dos riscos presentes na Empresa é feita priorização para que as vulnerabilidades que podem causar maior impacto sejam Analisadas e corrigidas conforme sua prioridade.

Uma forma de ser apresentada é como disposto abaixo, tornando fácil a visualização por parte dos gestores dos riscos presentes na Empresa.

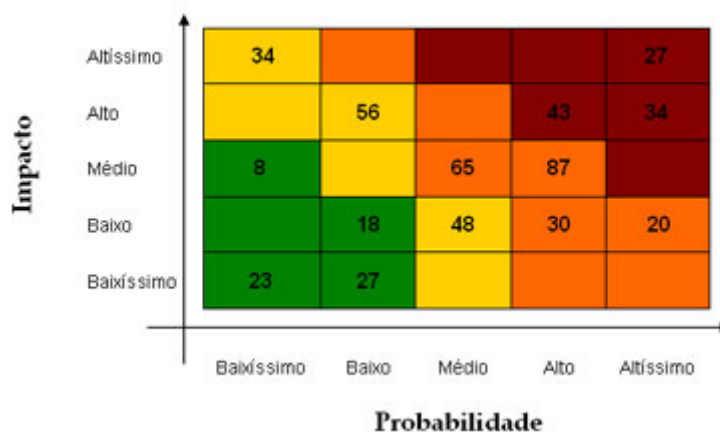


Figura 2 – Mapeamento de Vulnerabilidades

O natural é fazer com que as vulnerabilidades de alta probabilidade e alto impacto sejam “levadas” a um patamar de baixa probabilidade, como também as vulnerabilidades de risco médio (Alta probabilidade e baixo impacto) devem ser “levadas” para baixa probabilidade de ocorrência. Como na figura a seguir:

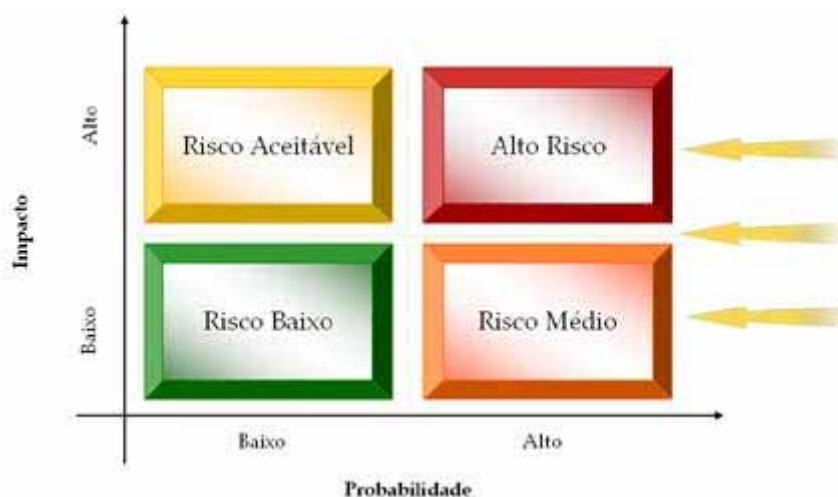


Figura 3 – Disposição dos riscos

Realizando uma Análise de Risco sua empresa terá respostas para perguntas como;

- 1- Qual o prejuízo financeiro se determinado ativo ficar indisponível ?
- 2- Qual a taxa de ocorrência de determinada ameaça ?
- 3- Qual a probabilidade de ocorrer novamente uma paralisação dos serviços?
- 4- Qual é o fator de risco ?
- 5- Qual impacto que pode ser causado ?
- 6- Qual impacto na imagem da Empresa ?
- 7- É possível conviver com determinado risco ?
- 8- Quais são as ameaças presentes na Empresa?
- 9- O que é necessário fazer e quanto gastar para reduzir os riscos ?

Toda e qualquer tomada de decisão futura relacionada a segurança da informação será baseada na Análise de Risco. Do plano de continuidade ao treinamento de pessoas haverá tomadas de decisões baseadas nela.

4. Plano de Continuidade

A **Análise de risco** esta diretamente ligada a **continuidade do negócio**, pois como descrito acima, a **análise de risco** vai identificar quais vulnerabilidades podem comprometer a continuidade. O Objetivo no plano de Continuidade é minimizar ou levar a zero as interrupções das atividades de seus colaboradores. A viabilidade, controles necessários e investimento financeiro devem estar de acordo com o apresentado na análise de risco. O investimento necessário para minimizar o risco de alguma ameaça não pode ser maior que o prejuízo calculado na análise de risco, nestes casos é importante definir procedimentos de como conviver com risco.

Quando aplicável, os documentos gerados são:

- Plano de Continuidade Operacional**
- Plano de Recuperação de Desastres**
- Plano de Administração de Crise**
- Plano para realização de Teste**

O Plano de Continuidade deve ser testado periodicamente a fim de garantir que sua informação seja recuperada dentro de um tempo máximo permitido

5. Classificar sua Informação

Um dos principais fatores para o sucesso da sua implantação é ter o conhecimento das informações que circulam na sua Empresa. Quem pode acessar, modificar ou excluir determinada informação ?

Por este motivo a **Foco Security** realiza o levantamento junto aos gestores da sua Empresa, identificando e classificando as informações durante seu ciclo de vida:

- **Armazenamento**
- **Manuseio**
- **Transporte**
- **Descarte da informação**

E normalmente classificando-as como:

- **Confidencial**
- **Restrito**
- **Interno**
- **Pública**

6. Política de Segurança da Informação

A **Política de Segurança** é a formalização de todos os aspectos considerados relevantes por uma organização para sua proteção, controle e monitoramento de seus recursos computacionais.

Também deve ser vista como um canal de comunicação entre usuários e o Comitê Corporativo de Segurança da Informação. A documentação gerada precisa explicar a importância da segurança para motivar as pessoas envolvidas a praticá-la.

7. Comitê Corporativo de Segurança da Informação

Já no início dos serviços, a **Foco Security**, estabelece junto a Empresa os responsáveis pelo Comitê Corporativo de Segurança da Informação.

O Comitê, basicamente, tem o objetivo de atuar com as áreas associadas, definir indicadores e metas, coordenar as medidas de segurança, avaliar os resultados, promover palestras (conscientização e manutenção da Política de Segurança), conduzir ações de auditoria e monitoramento, entre outras responsabilidades.

8. Teste de Invasão

O **Teste de Invasão** tem o objetivo de avaliar o grau de segurança oferecido pelos controles de segurança implementados em sua Empresa. Funcionando também, como um complemento à Análise de Risco, pois identifica suas vulnerabilidades. Os testes de invasão são divididos em:

Teste de invasão Interno: Como o próprio nome diz, é feito no ambiente interno da Empresa, levantando possíveis vulnerabilidades internas. Simulando o que seria possível realizar atuando como participante do ambiente. Várias pesquisas apontam que grande parte das tentativas de ataques são originadas dentro da Empresa. São verificadas falhas de segurança nas estações de trabalho, servidores, roteadores e aplicações internas entre outros.

Teste de Invasão Externo: Tem o objetivo de verificar o grau de segurança a tentativas externas de invasão. Visando principalmente conexões com a Internet e acesso remoto.

Em ambos os testes, são utilizadas técnicas de Engenharia Social, simulando de forma mais real técnicas utilizadas por pessoas que buscam coletar informações confidenciais de seu ambiente.

Características do relatório Teste de Invasão

- Informar detalhadamente as vulnerabilidades encontradas (Quais e como foram encontradas).

- Sugestões para correção das vulnerabilidades.

Permitindo aprimorar sua política de segurança de acordo com os resultados obtidos.

9. Campanha de Divulgação da Política de Segurança

A Campanha de Divulgação da Política de Segurança é uma das ferramentas responsáveis pelo sucesso da sua implantação.

Seu objetivo é divulgar a Política de Segurança da Informação na Empresa, conscientizando os colaboradores e prestadores de serviço para a Política de Segurança que está sendo implantada.

São desenvolvidas palestras de conscientização, cartas, e-mails, cartilhas e eventos objetivando o sucesso da implantação.

10. Avaliação de Segurança de Aplicações

A Avaliação de Segurança de Aplicações é um produto desenvolvido tanto para Empresas desenvolvedoras de Softwares quanto para Empresas que os utilizam em seus processos de negócio.

São realizados testes de segurança pela equipe técnica, visando identificar possíveis falhas de segurança tanto na visão de usuários, administradores ou agentes externos não autorizados.

A verificação pode ser realizada em sistemas em fase de projeto, desenvolvimento ou já em funcionamento em seu ambiente.

Ao final da avaliação de segurança é fornecido ao cliente relatório informando as falhas de segurança encontradas e sugestões para corrigi-las.

11. Política de Segurança implantada

Sua Empresa realizou a Análise de Risco, definiu o Plano de Contingência e implantou a Política de Segurança mas não foi auditada por ninguém ?

Como então garantir que estão sendo cumpridos os procedimentos definidos em sua **Política de Segurança** e se os controles implantados estão realmente funcionando ?

Pensando nestas situações, desenvolvemos o serviço de **verificação da sua política de segurança**, realizando testes de invasão interno, teste de invasão externo, verificando se o plano de continuidade está realmente funcional, realizando entrevistas com usuários e verificando se estes realmente foram bem treinados.

Ao final dos serviços sua Empresa terá certeza que sua implantação foi bem sucedida

12. Gerenciamento e Manutenção da sua Segurança

De nada adianta ter implantado a Política de Segurança sem garantir que esta vai realmente ser absorvida pela Empresa a longo prazo.

Na grande maioria das vezes a política de segurança tende a perder sua eficiência, pois ninguém verifica se está realmente sendo cumprida.

Pensando nisto, a **Foco Security**, desenvolveu o serviço de Gerenciamento e Manutenção da sua Segurança, onde são implementadas medidas que visam monitorar seu ambiente, identificar tentativas de invasão, garantir atualização da sua política de segurança, disponibilidade da sua informação e análise de risco periódicas.

Com a vantagem de receber mensalmente ou em tempo real relatórios com as atividades relacionadas à segurança da sua Empresa.

13. Monitoramento de sites.

É de conhecimento geral que seu site na Internet representa a imagem da sua Empresa.

Em alguns casos sua paralisação pode trazer grandes prejuízos financeiros.

Pensando nisto, que a **Foco Security** oferece o serviço de monitoramento de sites, que tem o objetivo de minimizar o risco deste sofrer alguma paralisação ou ser acessado por agentes não autorizados.

São realizados testes de invasão, relatórios periódicos e desenvolvido um plano de continuidade operacional.

14. Três principais motivos para contratar a Foco Security

1- Parceria estratégica com as **Faculdades Tancredo Neves**.

2- Modelo de negócio que possibilita elaboração de projetos com preços altamente competitivos.

3- Mão de obra qualificada e supervisão de projetos por profissionais e professores altamente qualificados.

15. Conclusão

No dias atuais a segurança das informações da sua empresa não pode ser mais tratada como diferencial, o impacto da falta de segurança esta totalmente ligado a posição da sua empresa perante o mercado, clientes, fornecedores e parceiros.

É necessário ter em mente que a análise de risco e controles devem ser revistos constantemente, as ameaças presentes no ambiente e fora dele mudam com velocidade espetacular, por este motivo também é necessário manter uma política que garanta a reavaliação dos riscos, a Analise de Risco deve ser feita com regularidade visando sempre identificar novos riscos.

Uma outra visão importante é relacionada ao investimento feito para reduzir o risco e retorno obtido, muitas empresas não conseguem enxergar o quanto a empresa deixara de perder com investimento em segurança. Muitas vezes isto ocorre pela não realização de uma analise de risco ou uma análise mal realizada. É muito importante mostrar nas projeções os prejuízos financeiros se uma determinada ação não for tomada.

É necessário mostrar ao gestor que determinado investimento em segurança trará benefícios e reduzirá despesas futuras. Também é necessário mostrar que determinados investimentos não são viáveis, investir mais do que as projeções de perda em um determinado ativo, muitas não é viável, o melhor e criar procedimentos para conviver com o risco.

Esperamos que este material tenha sido útil para você em alguma tomada de decisão.

16. Contato Comercial

Nosso contato comercial é realizado em parceria com a [Broker Serviços e Sistemas](http://www.brokeronline.com.br) (www.brokeronline.com.br), empresa com mais de 15 anos de experiência no mercado, cujo seu foco é fornecer soluções, prestar consultoria e serviços em desenvolvimento de sistemas. Esta parceria estratégica possibilita que a **Foco Security** centralize seus esforços em soluções para **Segurança da Informação**.

Se deseja um contato comercial, nosso atendimento é realizado pelo telefone: **(11) 3667-4466**

17. Sobre o conteúdo deste documento:

- Qualquer informação, crítica ou reclamação referente a este documento podem ser enviadas para o e-mail: atendimento@focosecurity.com.br

- As informações aqui contidas podem ser utilizadas desde que citada a fonte da seguinte forma:

Foco Security – www.focosecurity.com.br

Documento gerado por Hugo Ferreira Leitão