Aula 2

Segurança em Sistemas de Informação

Prof. Me. Luis Gonzaga de Paulo

A Organização da Segurança da Informação

Agenda

- Marcos regulatórios
- Política de segurança da informação
- Estratégias de segurança da informação
- Medidas de controle
- Governança e *compliance*

Contextualizando

- A ubiquidade da SegInfo
- A aparente complexidade que atrapalha
- Leis, normas, regras, padrões
- Boas práticas
- Assertividade

Marcos Regulatórios

- **Normas ISO**
- **Leis de alcance global**
- **Acordos internacionais**
- **Constituição brasileira**
- **Leis no Brasil**

- **As normas ISO são referências universais para diversas áreas do conhecimento, incluindo, também, a SegInfo**
- **Estabelecem padrões para diversos temas da SegInfo, tais como:**

- ✓ **a segurança em si**
- ✓ **os sistemas e métodos**
- ✓ **as certificações**
- ✓ **a auditoria**
- ✓ **as métricas**

- **No âmbito da SegInfo, as normas ISO mais conhecidas são as do conjunto 27000, voltadas para a prática da gestão de SegInfo. Porém, existem outras que visam atividades específicas, tais como:**

- ✓ **13335: GMITS**
- ✓ **14516: E-commerce**
- ✓ **15408: CC**
- ✓ **17994: Finance**
- ✓ **etc.**

- **A legislação de alcance global é voltada para um país, mas resulta em padrões, controles e medidas que afetam a diversos outros. São exemplos desse tipo de legislação:**

- ✓ **SOX**
- ✓ **HIPAA**
- ✓ **FISMA**
- ✓ **IFRS**
- ✓ **FATCA**
- ✓ **etc.**

- **A Constituição faz referências a aspectos da segurança da informação no capítulo 1, artigo 5º. Além disso, há leis sobre temas específicos:**

- ✓ **MPs 2200/01 e 2026/07**
- ✓ **Decreto 3714/01**
- ✓ **Leis 9609 e 9610/98**
- ✓ **Lei 12737/12**
- ✓ **Lei 12965/14 – Marco Civil da Internet**

Política de Segurança da Informação

- **Documento da organização**
- **Regras, padrões e práticas**
- **Normatização**
- **Orientação**
- **Informação**
- **Responsabilização**
- **Penalização**

- **A PSI abrange muito mais do que a TI, devendo endereçar a toda a organização, com o conhecimento de todos, considerando:**

- **os aspectos legais**
- **as necessidades do negócio**
- **aspectos técnicos e operacionais**
- **a evolução tecnológica**
- **capacitação e *compliance***

- **A PSI deve abordar aspectos críticos (exemplos: contratação e dispensa de pessoal; gerência de crises), orientando até mesmo em processos operacionais:**

- **quem faz?**
- **como faz?**
- **quando faz?**
- **onde faz?**
- **por que faz?**

Estratégias de Segurança da Informação

- **Menor privilégio**
- **Defesa em profundidade**
- **Ponto de estrangulamento**
- **Elo mais fraco**

- **Posição à prova de falhas**
- **Permissão/Negação padrão**
- **Diversidade da defesa**
- **Obscuridade**
- **Simplicidade**
- **Participação universal**

- **Menor privilégio: acesso, material e ferramentas apenas para a execução das atividades que competem à função (hierarquia):**

- ✓ **operador de caixa de supermercado → registro das compras**
- ✓ **cancelamento → supervisor ou gerente**

- **Defesa em profundidade: diferentes mecanismos de forma combinada. As defesas estão justapostas ou apresentadas em sequência ou diferentes níveis**

✓ **Exemplo**

❖ **Fechadura da porta do carro → chave de ignição → sensor de presença da chave → alarme**

- **Mecanismos bastante diferenciados**
- **Intuito: evitar o roubo do veículo**
- **Agem em sequência e em conjunto**

- **Ponto de estrangulamento: reduz ao mínimo os pontos de conexão e tráfego entre os ambientes da organização – áreas de menor e de maior proteção e segurança**

✓ **Aplica-se o máximo de medidas e mecanismos de segurança a esse ponto: monitoramento, vigia, retenção e contenção, vistoria etc.**

➢ **Exemplos**

❖ **Portaria de um edifício**

❖ **Portão de embarque no aeroporto**

❖ **Acesso à internet**

- **Elo mais fraco: o elemento de maior vulnerabilidade na escala de riscos ou o elemento mais visado, e que por isso mesmo demanda uma maior atenção e proteção**

- **Exemplos**
  - **Servidor**
  - ***Router***
  - ***Firewall / Proxy***
  - **Processos manuais**
  - **Intervenção humana**
  - **Pessoas**

- **Posição à prova de falhas: redução do perímetro de defesa para alvos de ataques em potencial (mais vulneráveis ou mais visados) para que recebam proteção máxima**

- **Exemplos**
  - **Cofre de banco**
  - **Data center**
  - **Fontes de energia**
  - **UTIs hospitalares**

- **Permissão ou negação padrão: é o controle de acesso e privilégios, com monitoramento e auditoria. Trata-se do uso de listas conhecidas como *black list* (não pode) ou *white list* (pode)**

- **Exemplos**
  - **Código de trânsito**
  - **Lista de convidados**
    - **Importante: *black list* não é o oposto de *white list***

- **Diversidade da defesa: uso de mecanismos diferentes no mesmo nível de proteção, reforçando os aspectos mais efetivos e reduzindo as deficiências de cada um**

- ✓ **Exemplos**
  - ❖ **Cerca eletrificada**
  - ❖ **Vigias humanos**
  - ❖ **Cães de guarda**
  - ❖ **Câmeras de monitoramento**
    - o **Todos no controle de acesso físico principal**

- **Obscuridade: segredo, ocultação. "O que os olhos não veem o coração não sente". Visa reduzir o interesse e combater a Engenharia Social, ocultando, por exemplo:**

- ✓ **nomes**
- ✓ **recursos**
- ✓ **arquivos**
- ✓ **técnicas usadas**
- ✓ **versões de *software***
- ✓ **e outras importantes referências**

- **Simplicidade: prima pela facilidade do aprendizado e uso frequente. Não é uma solução simplista, improvisada ou fraca, mas de rápida e fácil assimilação e execução**

- ✓ **Exemplos**
  - ❖ **Composição de senhas**
  - ❖ ***Clear desk* e *clear screen***
  - ❖ **Descarte de impressos**
  - ❖ **Atualização de antivírus**
  - ❖ **Execução de *backups***

- **Participação universal: atuação em conjunto de todos os envolvidos nos processos de segurança da informação e dos sistemas. Implicações:**

- ✓ **Nenhum processo ou iniciativa de segurança é suficientemente efetivo(a) por si só**
- ✓ **O comprometimento de todos é o que reforça a efetividade das medidas**

- ✓ **A segurança da informação é compromisso e responsabilidade de todos**

Medidas de Controle

- **Procedimentos, mecanismos e controles que dão suporte às estratégias**

- **Diversidade de elementos e controles diferenciados por:**
  - **segurança física**
  - **segurança lógica**

- ✓ **Segurança física: prevenção, detecção e combate às ameaças físicas, como:**

- **incêndios**
- **desabamentos**
- **descargas elétricas**
- **alagamento**
- **acesso indevido de pessoas**
- **forma inadequada de tratamento e de manuseio dos ativos e da informação**

- ✓ **Segurança lógica: prevenção, detecção e combate às ameaças "digitais", representadas principalmente por:**

- ***malware***
- **acessos remotos furtivos**
- ***backup* desatualizado**
- **cópias não autorizadas**
- **negação de serviço**
- **pichação de *site***
- **violação de senhas**

- **Os mecanismos de defesa devem ser compatíveis com as estratégias de defesa e em linha com a PSI e com o negócio, pois, caso contrário, podem:**

- **incorporar novos riscos**
- **causar o efeito contrário ao desejado**
- **comprometer os resultados da organização**

- **causar repulsa nos indivíduos**
- **estimular a sabotagem ou as ações contra a segurança das informações e dos sistemas**

Governança e *Compliance*

- Práticas da boa gestão
- Transparência
- Reconhecimento pelo público externo
- Confiabilidade
- ITIL
- COBIT

- A governança é resultado de um esforço comprovado e contínuo para a melhoria dos processos, produtos e serviços, detecção, correção e antecipação dos problemas, (...)

(...) do bom relacionamento e atendimento, da correta prestação de contas e garantia da confiabilidade

- O ITIL (*Information Technology Infrastructure Library*) é um guia para orientar o gerenciamento eficiente da área de TI para que esta possa prestar os seus serviços de maneira otimizada e eficaz. (...)

(...) É um conjunto de melhores práticas de gestão de TI que surgiu no final dos anos 80

- O COBIT (*Control Objectives for Information and Related Technology*) é um guia que propõe o nível de excelência na gestão de TIC. (...)

(...) É voltado para a gestão de TIC e recomendado pelo ISACA/ISACF, cujo objetivo é apoiar os gestores na avaliação do risco e no controle dos investimentos de TIC da organização

- Juntamente com esses dois *frameworks*, as normas ISO ajudam a estabelecer as condições para a organização atuar em conformidade com as leis, as normas, as boas práticas e as recomendações de governança, isto é, para que esteja em situação de *compliance*

Síntese

- Aplicação da segurança da informação e de sistemas
- Leis, normas, regulamentos e boas práticas
- Marcos regulatórios

- A política de segurança da informação e dos sistemas
- Estratégias de segurança
- Medidas de controle e proteção
- Governança e *compliance*

Referências de Apoio

- Casa Civil. Constituição da República Federativa do Brasil de 1988. Disponível em: <http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm>. Acesso em: 20/02/2016.
- DSIC. Quadro da Legislação Relacionada à Segurança da Informação e Comunicações. Disponível em: <http://dsic.planalto.gov.br/documentos/quadro_legislacao.htm>. Acesso em: 20/02/2016.

- PMI. A Guide to the Project Management Body of Knowledgement (PMBOK GUIDE). Project Management Institute, 2013.
- DE PAULO, W. L.; FERNANDES, F. C.; RODRIGUES, L. G. B.; EIDIT, J. Riscos e controles internos: uma metodologia de mensuração dos níveis de controle de riscos empresariais. Revista Contabilidade e Finanças, v. 18, n. 43, USP, São Paulo, jan./abr., 2007.
- GALVÃO, Michele da Costa. Fundamentos em Segurança da Informação. São Paulo: Pearson Education, 2015.
- ABNT. Segurança da Informação – Coletânea eletrônica. Rio de Janeiro: ABNT, 2014.
- IFRS. Informações – Termos Contábeis – IFRS. Disponível em: <http://www.contabeis.com.br/termos-contabeis/ifrs>. Acesso em: 10/02/2016.
- FISMA. Federal Information Security Management Act. Disponível em: <http://www.tiespecialistas.com.br/tag/fisma>. Acesso em: 10/02/2016.

- **LAPOLLA, M.; MARTINELLI, F.; SGANDURRA, D. A Survey on Security for Mobile Devices. IEEE Communications Surveys & Tutorials, v. 15, n. 1, first quarter of 2013: 446–471.**