TRIBUNAL DE CONTAS DA UNIÃO

Auditoria de Segurança da Informação

Secretaria de Fiscalização de Tecnologia da Informação

Harley Alves Ferreira

Novembro de 2009

Agenda

- ✓ Objetivos.
- ✓ Conceitos.
- ✓ Atributos da Segurança da Informação (SI).
- ✓ Como a SI é obtida?
- ✓ Controles de Segurança.
- ✓ Continuidade de Negócios.
- ✓ Auditoria de SI.
- ✓ Estudos de Casos.

Objetivos

- ✓ Conhecer conceitos atinentes à segurança da informação.
- ✓ Compreender a importância da segurança da informação no contexto organizacional.
- ✓ Ser apresentado a NBR ISO/IEC 27002 e como ela é utilizada como critério de auditoria.
- ✓ Identificar aspectos que devem ser abordados numa auditoria de segurança da informação.
- ✓ Discutir questões de auditoria relacionadas à auditoria de segurança da informação.

- ✓ Objetivos.
- ✓ **Conceitos.**
- ✓ Atributos da Segurança da Informação (SI).
- ✓ Como a SI é obtida?
- ✓ Controles de Segurança.
- ✓ Continuidade de Negócios.
- ✓ Auditoria de SI.
- ✓ Estudos de Casos.

Conceitos

- Informação
  - ✓ Conjunto de dados, resultado de processamento, manipulação e/ou organização, com algum tipo de significado e/ou valor.
  - ✓ Ela pode existir sob diversas formas como: armazenada eletronicamente, impressa ou escrita em papel, transmitida por conversas ou meios de comunicação.
  - ✓ A informação é um ativo essencial para os negócios de uma organização e, consequentemente, ela necessita ser adequadamente protegida (NBR ISO/IEC 27002:2005).

Conceitos

- Informação
  - ✓ Qual o valor da informação?
  - ✓ Na sociedade da informação e do conhecimento, ter informação é ter poder.
  - ✓ Como fonte de poder, a informação transformou-se no mais cobiçado e valioso bem da atualidade, passando a merecer tratamento especial.

Conceitos

- Riscos associados à informação

Incidentes

- Vírus
- Ataques (*Hackers*)
- Indisponibilidade
- Vazamento/Furto de informações
- Fraudes
- Invasão de *site* na Internet

Consequências

- Perda financeira
- Danos à imagem
- Processos legais
- Queda produtividade

Impacto no Negócio

- Queda na receita
- Aumento dos custos
- Perda de:
  - Oportunidades
  - Diferencial competitivo
- Diminuição de:
  - Confiança do investidor
  - Confiança do cliente
  - Confiança do cidadão

Conceitos

- Segurança da Informação
  - ✓ Visa proteger a informação de diversos tipos de ameaças, com os objetivos de garantir a continuidade dos negócios, minimizar possíveis riscos, proteger investimentos, preservar a confidencialidade de dados sensíveis, entre outros.
  - ✓ Busca garantir a continuidade do negócio da organização e minimizar os danos causados a ela, por meio da prevenção e redução dos impactos causados por incidentes/acidentes relacionados à segurança.
  - ✓ No âmbito da TI, ela não inclui apenas a segurança de dados, mas também a segurança dos sistemas, recursos e serviços.

- ✓ Objetivos.
- ✓ Conceitos.
- ✓ **Atributos da Segurança da Informação (SI).**
- ✓ Como a SI é obtida?
- ✓ Controles de Segurança.
- ✓ Continuidade de Negócios.
- ✓ Auditoria de SI.
- ✓ Estudos de Casos.

Atributos da SI

- Confidencialidade
  - ✓ Garantia de que a informação é acessível somente por pessoas autorizadas a terem acesso.
- Integridade
  - ✓ Salvaguarda da exatidão e completeza da informação e dos métodos de processamento. Garantia que esses somente sejam alterados por meio de ações planejadas e autorizadas.
- Disponibilidade
  - ✓ Garantia de que os usuários autorizados têm acesso à informação e aos ativos correspondentes quando requerido.

Atributos da SI

- Autenticidade
  - ✓ Garantia da veracidade da fonte das informações, sendo possível confirmar a identidade da pessoa ou entidade que presta informações, isto é, se ela é realmente quem diz ser.
- Não-repúdio
  - ✓ É a garantia que o emissor de uma mensagem ou a pessoa que executou determinada transação de forma eletrônica não poderá posteriormente negar sua autoria.
- Responsabilidade (*accountability*)
  - ✓ É a habilidade para manter pessoas ou entidades responsáveis por suas ações por meio do registro de seus atos.

- ✓ Objetivos.
- ✓ Conceitos.
- ✓ Atributos da Segurança da Informação (SI).
- ✓ **Como a SI é obtida?**
- ✓ Controles de Segurança.
- ✓ Continuidade de Negócios.
- ✓ Auditoria de SI.
- ✓ Estudos de Casos.

Como a SI é obtida?

- Análise de Riscos
  - ✓ Análise das ameaças, impactos e vulnerabilidades dos recursos de TI e da probabilidade de sua ocorrência.
  - ✓ Gastos com controle necessitam ser balanceados (Custo X Benefício).
  - ✓ Direciona e determina ações gerenciais a partir da identificação de requisitos de segurança.
  - ✓ Proporciona o estabelecimento de controles.
  - ✓ Análise de risco é responsabilidade do gestor. O auditor é responsável por avaliar a gestão do risco realizada pelo gestor e os controles implementados.

Como a SI é obtida?

- Estabelecendo requisitos de segurança
  - ✓ É fundamental que a organização identifique seus requisitos de segurança.
  - ✓ Fontes principais:
    - ✓ Análise de Risco dos Ativos de Informação.
    - ✓ Normas internas (PSI, classificação da informação).
    - ✓ Legislação vigente, estatutos, regulamentação e cláusulas contratuais (requisitos legais).
    - ✓ Conjunto particular (no contexto da organização) de princípios, objetivos e requisitos para o processamento da informação (objetivos de negócio).

Como a SI é obtida?

- Estabelecendo controles
  - ✓ Uma vez identificado os requisitos de segurança, podem ser selecionados e implementados controles que visem satisfazer esses requisitos.
  - ✓ Existirão situações onde a implementação de controles não será capaz de eliminar as vulnerabilidades identificadas, contudo poderá ser suficiente para reduzir os seus respectivos impactos ou probabilidade de ocorrência a um nível de risco aceitável.
  - ✓ Controles compensatórios também devem ser identificados. Exemplo: funções devem ser segregadas para evitar fraudes e erros, contudo isso pode não ser possível para organizações pequenas e, nesse caso, outra maneira de se alcançar o mesmo objetivo de controle poderá ser necessário (ex.: utilização de trilhas de auditoria para monitoramento de acessos e atividades por outra pessoa).

Como a SI é obtida?

- Implementação de controles por meio de:
  - ✓ Políticas
  - ✓ Práticas
  - ✓ Procedimentos
  - ✓ Pessoas
  - ✓ Estruturas organizacionais
  - ✓ Ferramentas de *software*

Como a SI é obtida?

- Fatores críticos de sucesso
  - ✓ Avaliação de riscos.
  - ✓ Política de segurança, com atribuição de responsabilidades.
  - ✓ Classificação da informação.
  - ✓ Enfoque para implementação da segurança que seja consistente com a cultura organizacional.
  - ✓ Comprometimento e apoio visível da administração.
  - ✓ Divulgação eficiente da segurança para todos os funcionários, proporcionando educação e treinamento adequados.
  - ✓ Monitoração.
  - ✓ Tratamento e resposta a incidentes.

Como a SI é obtida?

- Política de Segurança da Informação (PSI)
  - ✓ Prover à administração uma direção e apoio para a segurança da informação.
  - ✓ Estabelecer os princípios adotados pela organização para a distribuição, proteção, administração e supervisão dos recursos de informação.
  - ✓ Resolução da alta administração – "*top-down*".
  - ✓ Grande pilar de sustentação do ambiente informatizado, onde o fundamental é preservar os princípios básicos de segurança: integridade, disponibilidade, confidencialidade.

Como a SI é obtida?

- Política Corporativa de Segurança da Informação do TCU (PCSI/TCU) – Resolução-TCU nº 217, de 15 de outubro de 2008.
  - ✓ http://portal2.tcu.gov.br/portal/page/portal/TCU/comunidades/seguranca_informacao/normas_internas -

- Classificação da Informação no TCU - Resolução-TCU nº 229, de 11/11/2009.

- ✓ Objetivos.
- ✓ Conceitos.
- ✓ Atributos da Segurança da Informação (SI).
- ✓ Como a SI é obtida?
- ✓ **Controles de Segurança.**
- ✓ Continuidade de Negócios.
- ✓ Auditoria de SI.
- ✓ Estudos de Casos.

Controles de Acesso

- Princípios básicos

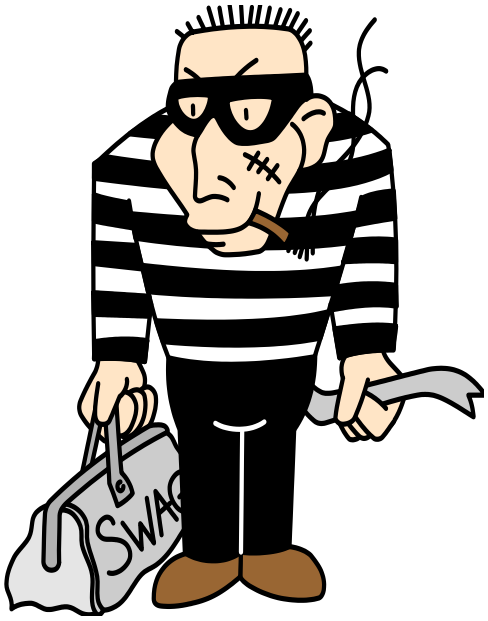
  - ✓ Definição da Política de Controle de Acesso (PCA). A PCA é o documento que especifica como os usuários são identificados e autenticados, além do seu nível de acesso aos recursos.

  - ✓ Segregação de funções: visa garantir que nenhuma ação individual poderá comprometer a segurança de um sistema ou obter acesso não autorizado aos dados.

  - ✓ Política do menor privilégio: requer que não será dado a um usuário ou processo mais privilégios que o necessário para execução de seu trabalho.

Controles Físicos

- Ameaças Físicas
  - ✓ Dano físico.
  - ✓ Furto.
  - ✓ Divulgação e cópia não autorizada de informações.
  - ✓ Sabotagem/Terrorismo.
- Ameaças Ambientais
  - ✓ Incêndio.
  - ✓ Água/Umidade/Secura.
  - ✓ Flutuações e cortes de energia.
  - ✓ Raios.
  - ✓ Temperaturas muito altas/baixas.



Controles Físicos

- Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização (ABNT NBR ISO/IEC 27002:2005)

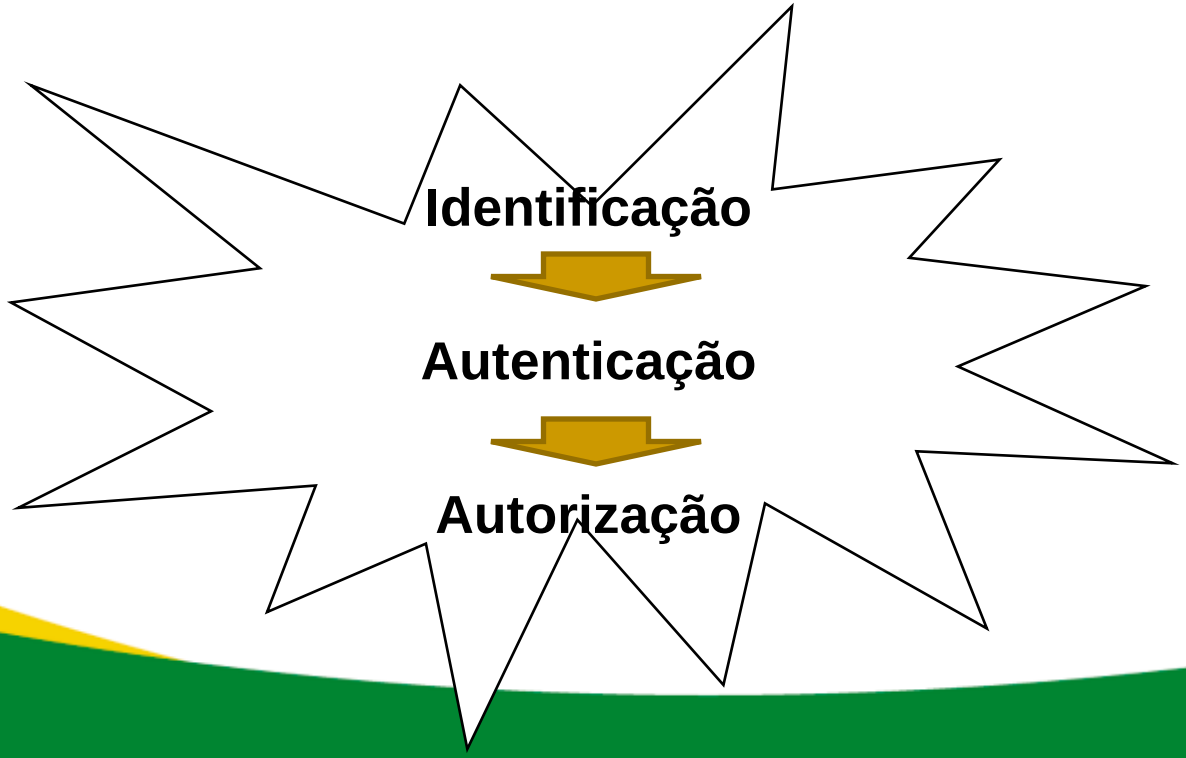
- Classificação dos Controles Físicos

  - ✓ **Controles de Acesso**: controles que impedem ou limitam o acesso físico (ex.: estabelecimento de perímetro de segurança, acesso de pessoas e veículos, cadeados, cofres, sala-cofre etc).

  - ✓ **Controles Ambientais**: visam proteger os recursos computacionais contra danos provocados por desastres naturais e por falhas estruturais (ex.: sistema de energia, de refrigeração, detectores e supressores de água e fogo, redundância, backup etc).

Controles de Acesso Lógico

- Controles de Acesso Lógico
  - ✓ Conjunto de medidas e procedimentos, administrativos ou intrínsecos aos *softwares*, responsável pela proteção dos recursos computacionais (dados, programas) contra tentativas de acesso não autorizadas.



Controles de Acesso Lógico

- Possíveis consequências de acessos não autorizados
  - ✓ Divulgação não autorizada.
  - ✓ Alteração não autorizada.
  - ✓ Perda de integridade do sistema.
  - ✓ Perda financeira.
  - ✓ Descumprimento de obrigações legais.
  - ✓ Perda de competitividade ou credibilidade no mercado.
  - ✓ Interrupção das atividades do negócio.

Controles de Acesso Lógico

- Identificação dos usuários
  - ✓ Códigos de identificação única
  - ✓ Método mais comum é o uso de uma credencial (ID ou *login*)
- Autenticação dos usuários
  - ✓ Envolve algo que o usuário
    - ✓ É – impressão digital, identificação de retina, DNA etc
    - ✓ POSSUI – cartão de identificação, *token* etc
    - ✓ CONHECE – senha, frase, PIN etc
  - ✓ Método mais comum é a senha

Controles de Acesso Lógico

- Controle de senhas
  - ✓ Regras de composição (exigência de senhas de qualidade)
  - ✓ Tamanhos máximo e mínimo
  - ✓ Tempo de validade
  - ✓ Histórico para não reutilização
  - ✓ Armazenada de forma de *hash* (via de mão única) ou criptografada
  - ✓ Alocação inicial
  - ✓ Senhas de demissionários
  - ✓ Orientação aos usuários

Controles de Acesso Lógico

- Outros controles
  - ✓ Restrições a sessões concorrentes (mesmo usuário)
  - ✓ Limitação do horário de trabalho
  - ✓ Tentativas de acesso controladas
  - ✓ Proteção de tela automática
  - ✓ Acesso a terminal específico

- Política de Controle de Acesso (PCA)
  - ✓ Define procedimentos e controles de acesso (ex: regras para concessão/desligamento)

- ✓ Objetivos.
- ✓ Conceitos.
- ✓ Atributos da Segurança da Informação (SI).
- ✓ Como a SI é obtida?
- ✓ Controles de Segurança.
- ✓ **Continuidade de Negócios.**
- ✓ Auditoria de SI.
- ✓ Estudos de Casos.

Continuidade de Negócios

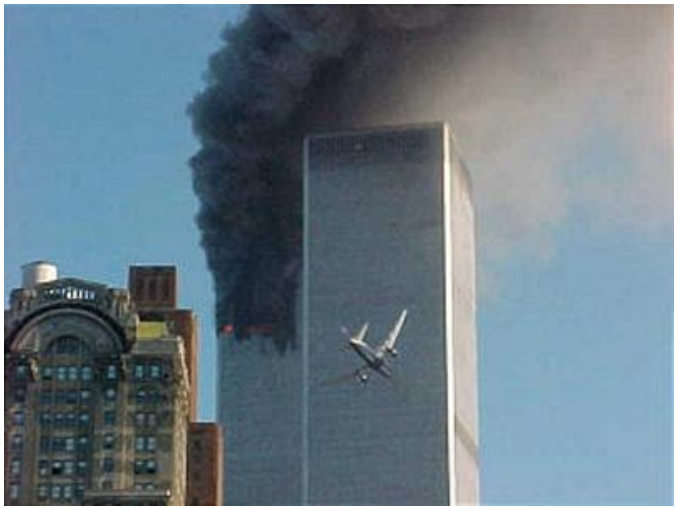
- ✓ A Gestão da Continuidade do Negócio tem por objetivo “não permitir a interrupção das atividades do negócio e proteger os processos críticos contra efeitos de falhas ou desastres significativos, e assegurar a sua retomada em tempo hábil, se for o caso” (NBR ISO/IEC 27002:2005, item 14.1).

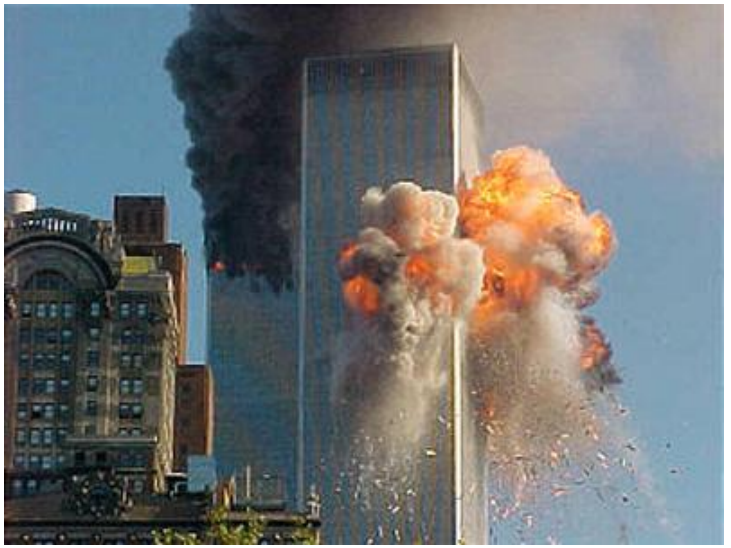
Continuidade de Negócios

- De cada cinco empresas que tiveram interrupção nas suas operações por uma semana, duas fecham as portas em menos de três anos (fonte: *Disaster Recovery Institute*)

- Impacto por interrupção (fonte: Universidade do Texas)
  - Perda de 0,5% da posição do mercado a cada 8 horas parada.
  - 3 anos para recuperar 0,5 % da sua posição no mercado.

Continuidade de Negócios

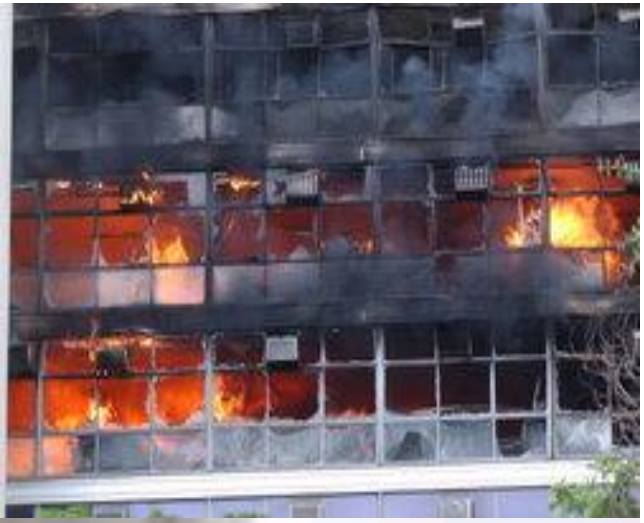


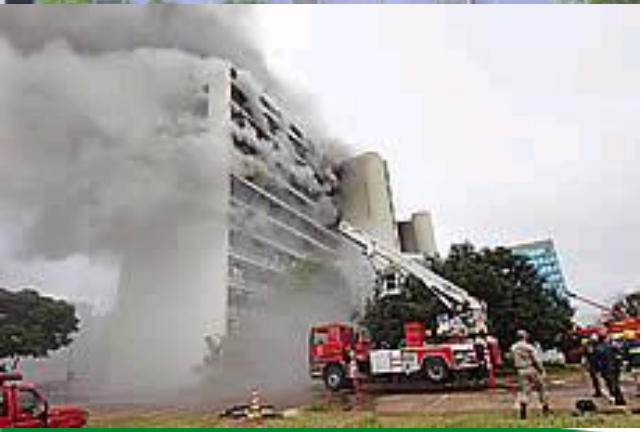


Continuidade de Negócios

- Lições do WTC – 2001
  - ✓ empresas sumiram do mapa.
  - ✓ quem tinha um Plano de Continuidade de Negócios (PCN), conseguiu continuar operando (maioria dos bancos):
    - ✓ empresas que optaram por apenas instalações alternativas de TI passaram por dificuldades para retomar operações.
  - ✓ todos os riscos devem ser objetivo de análise, independente de sua probabilidade (ex.: terrorismo).
  - ✓ foco do PCN: capital intelectual e instalações.
  - ✓ seus clientes/usuários/funcionários necessitam de informações ("*caos center*").
  - ✓ PCN incompleto e ambiente desatualizado dificultaram retomada rápida de atividades.
  - ✓ Usuários desconheciam o PCN: pessoas e testes são críticos.

Continuidade de Negócios





- Incêndio INSS - Brasília (27/12/2005)
  - ✓ 4º a 9º andares destruídos.
  - ✓ destruição de 104 processos de débitos tributários.
  - ✓ prejuízos de até R$ 10 Bilhões, segundo Anprev (Associação Nacional dos Procuradores da Previdência).
  - ✓ somente se cria grupo para elaborar plano de contingência em 29/12/2005 (Portaria 3.032).

Continuidade de Negócios

- Exemplo de deficiências na gestão da continuidade de negócio:

  - ✓ “Convivendo com total falta de recursos ou planos de contingência, a atual Diretoria [...] foi alarmada pela ocorrência do dia 19/07/2005, quando uma falha nos equipamentos de processamento centralizado provocou a paralisação [da entidade] por mais de 20 horas, gerando danos a imagem e causando prejuízos financeiros à instituição.” (TC 026.196/2007-9)

Continuidade de Negócios

- Mais um exemplo de deficiências na gestão da continuidade de negócio:

  - ✓ “Obteve-se a informação que, devido a um vírus, houve uma paralisação na rede [...] por mais de duas semanas, o que comprova que o Plano de Contingência [...] remetido [...] não tem aplicabilidade efetiva.” (TC 026.200/2007-3)

Plano de Continuidade de Negócios

- Plano de Continuidade de Negócios (PCN)

  - ✓ É o desenvolvimento preventivo de um conjunto de estratégias e planos de ação de maneira a garantir que os serviços essenciais sejam devidamente identificados e preservados após a ocorrência de um desastre.

  - ✓ É o conjunto de planos/programas, onde encontram-se detalhados os procedimentos a serem seguidos pelos colaboradores por ocasião de ocorrência de eventos que possam afetar algum componente e, consequentemente, o processo de negócio por ele suportado.

Plano de Continuidade de Negócios

- Eventos contemplados no PCN
  - ✓ Falha humana.
  - ✓ Falha de componentes de TI / comunicações.
  - ✓ Interrupção da energia elétrica.
  - ✓ Fenômenos da natureza (inundação, furacão, terremoto, maremoto etc).
  - ✓ Fogo, explosão, raios.
  - ✓ Distúrbio civil (greve etc).
  - ✓ Vírus, Acesso indevido, Roubo.
  - ✓ Ataque, sabotagem, vandalismo.
  - ✓ Explosão de bomba / avião / terrorismo.

Plano de Continuidade de Negócios

- Considerações em uma auditoria
  - ✓ Se a organização não tiver um plano, avaliar o grau de risco e determinar se a opção por “não fazer nada” é justificável.
  - ✓ Um requisito mínimo é a existência de uma estratégia de recuperação.
  - ✓ Existindo um plano, utilizar os procedimentos de auditoria associados para verificar se este é exequível, se está atualizado, e se o pessoal está treinado para executá-lo.
  - ✓ Avaliar conformidade com a ABNT NBR ISO/IEC 27002:2005 e ABNT NBR 15999.

- ✓ Objetivos.
- ✓ Conceitos.
- ✓ Atributos da Segurança da Informação (SI).
- ✓ Como a SI é obtida?
- ✓ Controles de Segurança.
- ✓ Continuidade de Negócios.
- ✓ **Auditoria de SI.**
- ✓ Estudos de Casos.

Auditoria de Segurança da Informação

- ✓ É avaliado se a gestão da segurança da informação, o controle dos ativos e os riscos envolvidos são considerados de forma efetiva pela organização. A auditoria de SI visa avaliar a gestão da organização com relação à segurança.
- ✓ Aborda aspectos de confidencialidade, integridade e disponibilidade embutidos nos conceitos de segurança lógica e física.

Auditoria de SI

Aspectos abordados:

Comitês diretivos e deliberativos, políticas e normas, pessoas, responsabilidades, treinamento, identificação e classificação de ativos, classificação da informação, identificação e avaliação de riscos, gerência de problemas e incidentes, plano de continuidade de negócios, perímetro de segurança, equipamentos e instalações, gerenciamento e controle de acesso lógico, auditoria, conformidade.

Auditoria de SI

- Escopo de uma Auditoria de SI

  - ✓ Identificação e avaliação de controles que afetam a segurança da informação.

  - ✓ Poderá ser feita no contexto macro, envolvendo aspectos que envolvem toda a organização ou apenas considerando informações, sistemas, recursos, processos e serviços específicos.

Auditoria de SI

- Normas utilizadas
  - ✓ Decreto n.º 3.505/2000 – Estabelece diretrizes gerais para definição da Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.
  - ✓ Decreto n.º 4.553/2002 – Dispõe sobre a salvaguarda de dados, informações, documentos e materiais sigilosos de interesse da segurança da sociedade e do Estado, no âmbito da Administração Pública Federal.
  - ✓ Instrução Normativa Gabinete de Segurança Institucional da Presidência da República (GSI) nº 1, de 13 de junho de 2008 – Orienta as entidades da Administração Pública Federal quanto a questões relativas à segurança da informação.

Auditoria de SI

- Padrões utilizados
  - ✓ ABNT NBR ISO/IEC 27002:2005 (Código de Prática para a Gestão da Segurança da Informação).
  - ✓ ABNT NBR 15999 (Gestão de Continuidade de Negócios).
  - ✓ Cobit (*COntrol, governance and audit for Business Information and related Technology*).

Auditoria de SI

Objetivo de controle: assegurar que a organização define e estabelece diretrizes e responsabilidades pela segurança da informação e gestão de riscos.

Possíveis questões de auditoria:

- ✓ Há uma Política de Segurança da Informação formalmente aprovada e em vigor?
- ✓ Essa política define de forma suficiente os princípios que norteiam a gestão de segurança de informação e seus respectivos responsáveis?
- ✓ O ente aplica e divulga internamente essa política?
- ✓ O ente possui um Gestor de SI?
- ✓ A entidade instituiu um Comitê de Segurança da Informação e Comunicações? (Comitê SI / TCU – Portaria-TCU nº 277, de 18/11/2008)

Auditoria de SI

Critérios:

- ✓ Artigo 5º da Instrução Normativa GSI nº 1, de 13 de junho de 2008.
- ✓ Item 5.1 da NBR ISO/IEC 27002:2005.
- ✓ PO4.8 e PO6.1 do Cobit 4.1.

Possíveis achados:

- ✓ Baixo comprometimento do ente quanto à SI.
- ✓ Política de Segurança da Informação inexistente, informal, insuficiente, não aplicada ou não divulgada (não efetiva).
- ✓ A entidade não possui um Gestor de Segurança da Informação ou um Comitê Gestor de Segurança da Informação e Comunicações.

Auditoria de SI

Objetivo de controle: assegurar que existam procedimentos de controle de acesso com o objetivo de proteger equipamentos, sistemas, rede e arquivos de dados, de forma sistematizada e gerenciada.

Possíveis questões de auditoria:

- ✓ Os controles de acesso físico concorrem para proteger o ambiente de produção?
- ✓ Existem regras que disciplinam o acesso à informação?
- ✓ O ente possui regras definidas de controle de acesso lógico que dificultem o uso indevido das informações?
- ✓ As políticas de controle de acesso são suficientes, além de serem seguidas e aplicadas?

Auditoria de SI

Critérios:

- Acórdãos nos 2.023/2005, item 9.1.3 e 71/2007, item 9.2.7, todos do Plenário-TCU
- Item 11.1.1 da NBR ISO/IEC 27002:2005.
- PO6.1, DS5.3, DS5.4 e DS12.3 do Cobit 4.1.

Possíveis achados:

- Falta de uniformização e de procedimentos formalizados para acesso aos sistemas informatizados (incluindo a concessão, a revisão periódica e a revogação de acesso).
- Falhas nos procedimentos de entrada dos sistemas e de acesso físico aos ambientes de produção.
- Falhas no gerenciamento das senhas de usuários.
- Não são estabelecidas regras para formação de senhas e nomes de usuários.

Auditoria de SI

Objetivo de controle: certificar-se de que fragilidades, falhas e incidentes relacionados à segurança da informação são notificados, registrados e devidamente gerenciados, permitindo a tomada de ação corretiva.

Possíveis questões de auditoria:

- ✓ Os incidentes, as falhas e as fragilidades são comunicados por um canal único, apropriado, conhecido, acessível, disponível e utilizado por todos os clientes de TI?
- ✓ Os incidentes e falhas de segurança são tempestivamente identificados, estancados e corrigidos?

Auditoria de SI

Critérios:

- Artigo 5º, inciso V, da Instrução Normativa GSI nº 1, de 13 de junho de 2008.
- Itens 13.1 e 13.2 da NBR ISO/IEC 27002:2005.

Possíveis achados:

- Ausência de registros de incidentes de segurança.
- Indefinição sobre quem são as pessoas responsáveis pelo tratamento de incidentes.
- Os incidentes de segurança não são tratados.
- As falhas identificadas não são corrigidas.

Auditoria de SI

Objetivo de controle: certificar-se de que os riscos de TI são identificados, avaliados e tratados

Possíveis questões de auditoria:

- ✓ É efetuada análise de riscos na área de TI?
- ✓ A análise de riscos é constantemente atualizada?

Auditoria de SI

Critérios:

- ✓ CF, art. 37, caput (princípio da eficiência)
- ✓ NBR ISO/IEC 27002:2005, item 4 - Análise/avaliação e tratamento de riscos
- ✓ Cobit 4.1

  PO9.4 Avaliação de riscos

Possíveis achados:

- ✓ Inexistência de um processo formal de análise de riscos de TI

Auditoria de SI

Objetivo de controle: assegurar que a organização possui mecanismos sistematizados de retorno à normalidade em casos de incidentes

Possíveis questões de auditoria:

- ✓ Há procedimentos definidos para retorno à normalidade em casos de contingência?
- ✓ Os procedimentos são divulgados, conhecidos e testados periodicamente?
- ✓ Há um Plano de Continuidade do Negócio compatível com as necessidades operacionais do ente?
- ✓ Esse plano define quem são as pessoas e quais são os procedimentos chaves de continuidade do negócio?

Auditoria de SI

Critérios:

- Princípio da Continuidade dos Serviços Públicos.
- Art. 10, inciso IX, Lei nº 7.783/89 (processamento de dados ligados a serviços essenciais).
- Art. 22 da Lei nº 8.078/90 (fornecimento de serviços essenciais).
- Acórdão nº 71/2007-TCU-Plenário, item 9.2.14.
- Item 14 e subitens da NBR ISO/IEC 27002:2005.
- ABNT NBR 15999 (Gestão de Continuidades dos Negócios).
- DS4 e subitens do Cobit 4.1.

Auditoria de SI

Possíveis achados:

- ✓ Inexistência de Plano de Continuidade de Negócios.
- ✓ Ausência de área específica para lidar com incidentes e contingências.
- ✓ O plano não é conhecido.
- ✓ Treinamentos insuficientes.
- ✓ O plano não é testado e atualizado periodicamente.
- ✓ O plano é inexequível.
- ✓ A informação não é classificada segundo sua relevância, criticidade e necessidade de sigilo.
- ✓ Ausência de políticas ou procedimentos de back-up.

- ✓ Objetivos.
- ✓ Conceitos.
- ✓ Atributos da Segurança da Informação (SI).
- ✓ Como a SI é obtida?
- ✓ Controles de Segurança.
- ✓ Continuidade de Negócios.
- ✓ Auditoria de SI.
- ✓ Estudos de Casos.

Infraero

- Por quê?
  - ✓ Levantamento do TCU constatou que a Infraero conta com uma série de sistemas informatizados de arrecadação que não foram auditados/avaliados pela Auditoria Interna.

- Objetivo
  - ✓ Avaliar os aspectos de segurança dos principais sistemas informatizados pertinentes ao processo de arrecadação de receitas da Empresa Brasileira de Infra-Estrutura Aeroportuária - Infraero.

Infraero

- Problemas identificados (Acórdão nº 1092/2007 – TCU - Plenário)
  - ✓ Não realização de inventário e classificação de ativos de informação.
  - ✓ Inexistência de uma Política de Controle de Acesso (PCA).
  - ✓ Ausência de procedimentos formalizados para concessão e revogação de acessos aos sistemas.
  - ✓ Falhas nos gerenciamentos das senhas dos usuários.
  - ✓ Falta de conscientização dos funcionários quanto à confidencialidade das senhas.
  - ✓ Inexistência de Plano de Continuidade do Negócio.

Infoseg

- Por quê?
  - ✓ Auditoria operacional realizada durante o exercício de 2004 pelo TCU no programa Sistema Único de Segurança Pública (SUSP) identificou que havia problemas enfrentados pela Senasp e pelos estados na implantação do Infoseg.
- Objetivo
  - ✓ Avaliar aspectos relacionados à segurança e à consistência das informações gerenciadas pelo sistema.

Infoseg

- Problemas identificados (Acórdão n 71/2007 – TCU – Plenário)
  - ✓ Inexistência de PSI.
  - ✓ Falhas na Política de Controle de Acesso (PCA).
  - ✓ Inexistência de Plano de Continuidade do Negócio (PCN).
  - ✓ Gestão insatisfatória das cópias de segurança.
  - ✓ Deficiências na segurança física da gerência do Infoseg.
  - ✓ Indefinição dos proprietários de alguns ativos.
  - ✓ Falhas nos contratos de locação de mão-de-obra quanto à SI.
  - ✓ Insuficiência de trilhas de auditoria.
  - ✓ Inexistência de controles compensatórios para as operações dos administradores do sistema (DBA).

Reportagem na TV (SBT)

Obrigado!

Harley Alves Ferreira