Notas SGR

Slide 1:

Segurança da informação:
- informação são dados ordenados de forma a fazerem sentido
- Informação como sendo um ativo
- Pode ser informação por visão/multimedia (CCTV e espaços públicos)
- Informação por via áudio / oral (sistemas de de encriptação da voz)
- INformação impressa (watermarks para certificação, secure printing)
- Informação em formato digital (Discos cifrados,VPN,VLAN)

Iso 27001: descreve como se deve implementar/gerir um ISMS.

ISMS: Um information security management system, um sistema de gestão que contém procedimentos, políticas para garantir a segurança da informação, preservando o CIA.

Information Security: preserva CIA da informação.

Gestão da Segurança de informação na organização:
- Garantir a CIA
- Reduzir riscos para o negócio e minimizar o impacto de incidentes.

A ameaça usa a vulnerabilidade para causar um risco.

Ameaça: Qualquer coisa com potencial de causar danos
Risco: Probabilidade de algo mau acontecer.
Vulnerabilidade: Fragilidade que pode causar danos à informação.

Vulnerabilidades:
- Não ha IDS
- Não ha firewall
- Informação em claro
- Sistemas não redundantes etc.

Risco:
- Roubo de informações
- Perda de dados
- Corrupção de dados
- Personificação
- Conversas em locais públicos
- Documentos em suporte físico

Ameaças:

- Hacking
- Espionagem
- Inundação
- Avaria
- Falha energética.

Abordagem integrada à Segurança:

- Para se conseguir garantir a segurança de um sistema de informação de forma integrada
- Normas e procedimentos (políticas de segurança por ex)
- Sistemas e aplicações (testes e acompanhamento)
- Infra-estrutura (Mecanismos de controlo e monitorização)
- Acesso físico (acesso a edifícios, e controlo de acesso a zonas)

Para criar uma política de segurança é preciso definir a estratégia, adequar a estrutura organizacional, documentar, implementar a política de segurança e certificar.

Para definir a estratégia:

- Âmbito
- Requisitos: (preservar CIA)
- Identificação de riscos

Para adequar a estrutura:

- Comité de segurança (pessoas de gestão e elementos de nível operacional)

A política:

- Deve focar na segurança organizacional, controles de acessos a comunicações e dados, procedimentos e responsabilidades etc.
- Garantir alinhamento da política de segurança por auditorias externas porque os requisitos do negócio podem alterar

Certificação da política de segurança

Slide 2:

Normas e legislação aplicável:

Recurso a normas e boas práticas permite utilização de metodologias testadas e comprovadas.

Requisitos:

- Normativos
- Legais
- Contratuais

O conhecimento e adoção de requisitos legais permite cumprimento da lei, assegurando a legalidade.

Introdução à ISO 27001:

- descreve como gerenciar a segurança da informação em uma organização, tendo como foco a preservação da CIA da informação
- Cláusulas 4 a 10 são as que importam

ISO/IEC 27002:2013:

- é desenhada para implementar controlos no processo de implementação do ISMS

A ISO 27001:

- contém requisitos para a implementação de um ISMS

Modelo PDCA aplicado ao ISMS:

- Plan : estabelecer políticas, objetivos e procedimentos para melhorar o ISMS.
- Do : Implementar as políticas e procedimentos
- Check : Verificar quão efetivo foi a melhoria ao ISMS
- Act : Melhorar o ISMS

ISO 27001 Sistema de Gestão:

- Requisitos para um ISMS, para ser certificado pela ISO 27001.

Sistema de Gestão:

- Contexto da organização
- Liderança
- Planeamento
- Suporte
- Operação
- Avaliação de desempenho
- Melhoria

Anexo A:

- Controlos

Implementação dos controlos: ISO 27002

Introdução á gestão de risco (27005):

- o risco é a probabilidade de algo mau vir a acontecer e causar danos a informação
- O risco é avaliado de acordo com a probabilidade, impacto, controlos existentes etc.
- Ameaças e Vulnerabilidades ISO 27005

Avaliação de risco:

- Várias fórmulas para calcular o risco.
- Feito através de matrizes de risco (probabilidade, impacto)

Tratar os riscos:

- Aceitar os riscos

- Evitar os riscos (Desligar serviço)
- Transferir os riscos (seguradoras)
- Mitigar riscos.

Slide 3:

Introdução á gestão de continuidade de negócio:

- A gestão da continuidade de negócio faz parte da gestão de risco de uma organização
- Leva à produção de planos e procedimentos que permitam às organizações responder a incidentes de maneira eficaz.
- Iso 22301
- É preciso identificar processos críticos, eventos de uma eventual descontinuação para permitir responder a incidentes de maneira eficaz.

Avaliação e gestão de riscos vs gestão de risco:

- A avaliação é só uma vez
- Gestão contém uma avaliação e monitorização constante do risco, implementações de controles etc. é um processo contínuo.

A gestão de risco tem como objetivo:

- Controlar os riscos de forma a que seja o menos possível acontecer algum problema, mantendo assim os sistemas em segurança.
- Permite tomadas de decisões que justifiquem investimentos.

A gestão de risco é implementada sobre novos e antigos processos e sistemas implementados.

A avaliação de risco deve ser feita nas fases iniciais do projeto, porque mais tarde vão ter custo mais alto.

Avaliação dos riscos:

- Primeiro descubra as ameaças, formas de mitigar os riscos e análise custo benefício, inerentes a um projeto.
- Iso 31000 e 27005

Como quantificar o risco:

- Valores numéricos (quantitativo): números
- Qualitativo através de níveis. : Low, Medium, High
- Mista

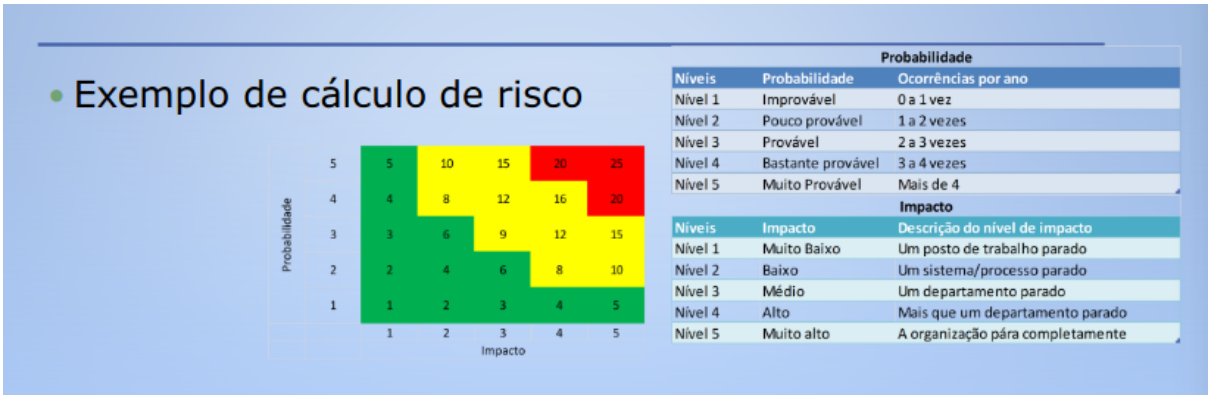
Formas de calcular o risco:

- Devem ser sempre aplicadas de maneira igual a tudo.
- Fórmulas = Impacto * probabilidade
- Devem ser quantitativos no melhor dos casos.

Os fatores de risco:

- Probabilidade
- Impacto

São considerados 5 níveis numerados de 1 a 5 que torna quantitativo.



Probabilidade		
Níveis	Probabilidade	Ocorrências por ano
Nível 1	Improvável	0 a 1 vez
Nível 2	Pouco provável	1 a 2 vezes
Nível 3	Provável	2 a 3 vezes
Nível 4	Bastante provável	3 a 4 vezes
Nível 5	Muito Provável	Mais de 4

Impacto		
Níveis	Impacto	Descrição do nível de impacto
Nível 1	Muito Baixo	Um posto de trabalho parado
Nível 2	Baixo	Um sistema/processo parado
Nível 3	Médio	Um departamento parado
Nível 4	Alto	Mais que um departamento parado
Nível 5	Muito alto	A organização pára completamente

Formas de estimar a probabilidade:
Dados Internos:

- Utilizar o histórico de incidentes até a data.
- Experiência dos colaboradores
- Através de questionários e discussões em grupo.

Dados externos:

- Dados partilhados por organizações

Análise e avaliação de risco de acordo com o 27005:

- Estabelecer contexto e limites
- Definir níveis de avaliação a serem utilizados e Risco mínimo aceitável
- Identificar os ativos.
- Valorizar os ativos
- Identificar ameaças, vulnerabilidades, controles existentes etc.
- Estimar riscos operacionais e financeiros
- Plano de tratamento dos riscos

Tratamento dos riscos (Iso 27005):

- Assumir o risco (arriscar)
- Evitar o risco (desligando o sistema)
- Transferência de risco (seguradoras)
- Aplicação de controlos ou mitigar riscos.

Risk Mitigation Checklist:

- Each proposed risk mitigation should be examined to check if the mitigation is worth it, se vale é effective o suficiente, se é prática de implementar etc.

Fluxo de aceitação de riscos:

- Os passos que se deve fazer para verificar se vale a pena considerar o risco para a avaliação.

Controlos de segurança:
- Deve resultar de avaliação de risco.
- Na iso 27001 existem controlos.
- Podem ser agrupados:
- Controlos tecnológicos de suporte (administração da segurança e proteção de sistemas)
- Controlos técnicos preventivos (autenticação, autorização, controlos de acesso, proteção comunicações)
- Controles de detecção (detectar violação de políticas com auditorias, vírus detection, IDS/IPS etc).

- Controlos de Gestão e Organizacionais preventivos (programas de formação e sensibilização dos operadores)
- Controlos de Gestão e Organizacionais Detecção (Realizar auditorias periódicas)
- Controlos de Gestão e Organizacionais Recuperação (Estabelecer o plano de continuidade de negócio)

- Controlos Operacionais Preventivas (Mecanismos de backup)
- Controlos Operacionais Deteção (sistemas de vigilância)

Slide 4:

Abordagem integrada a segurança:
- Só se consegue atingir a segurança de informação através de uma forma integrada:
- Normas e procedimentos
- Sistemas e aplicações
- Infraestrutura física e lógica.

Para as normas e procedimentos é necessário definir políticas de segurança.
O modelo de segurança integrado está na 27002.

Definição de política de segurança:
- Uma política de segurança deverá ser aprovada pela direção da organização
- Contém um conjunto de regras que devem ser seguidas, normas e procedimentos.
- Devem ser revistas periodicamente.

No modelo de segurança integrado:
- Segurança e gestão de RH (verificar credenciais)
- Organização da segurança (Segregação de funções)
- Gestão de ativos (inventário de recursos)
- Controlos de acesso à informação (Regras de controlo, Clean Desk, Controlos de acessos)
- Criptografia dos dados (gestão de chaves)

- Segurança física e ambiental (manutenção e perímetro)
- Segurança de comunicações

Processo de análise de risco FRAAP:
- Serve para análise de avaliação de risco
- É fácil, rápido e envolve a organização.
- Para o cálculo do risco é usado o método qualitativo.

Toda a equipa é envolvida para detectar ameaças, níveis de risco e possíveis controles a aplicar.

Vantagens:
- É rápido
- Envolve o responsável do negócio
- Permite encontrar controlos apropriados

Equipa envolvida:
- Responsável pelo negócio
- Gestor do projeto
- Facilitador
- Escriba
- Especialistas (Users, IT)

O Facilitador é aquele que guia a reunião, fala com o grupo para tentar identificar ameaças, controles e níveis de risco. Deve manter todos focados no tema e controlar o tempo, encorajar a participação de todos e regular a reunião.

O Escriba documenta toda a reunião, ameaças, controlos e riscos.

Os especialistas relacionados com o objeto em análise devem conhecer o sistema utilizá-lo e devem conhecer vulnerabilidades e ameaças.

3 passos no FRAAP:
- Pré-FRAAP
- FRAAP
- Pós-FRAAP

Antes de iniciar deve existir um programa de sensibilização onde se dá a conhecer o processo do FRAAP à empresa.

É preciso garantir o envolvimento dos participantes.

Na reunião pré-fraap deve incluir:
- Gestor de negócios
- Facilitador
- Escriba

Resultados esperados:

- Pré-triagem
- Definição de âmbito (o que vamos analisar)
- Diagrama do sistema (diagrama do sistema a analisar)
- Equipa a incluir
- Requisitos para a reunião FRAAP (onde vai ser, a que horas etc)
- Definições (o que é uma ameaça, impacto, risco etc)
- Mini-brainstorming (descobrir ameaças do CIA)

FRAAP:
- Demora 4h
- Envolve todos os membros da equipa

Resultados esperados:
- Identificação de ameaças, controlos existentes, cálculo de riscos, identificação de novos controlos, cálculo de risco residual (o do fim).
- Desencorajar o uso de telemóveis.

Primeiro o responsável apresenta o facilitador
Depois o facilitador apresenta a agenda e explica o processo.
Review scope statement.
Percorrer de ponta a ponta de forma a perguntar possíveis ameaças para CIA.
Depois de se esgotarem o facilitador pode dar ideias.
Depois pausa
Depois controlos existentes
Depois estabelecer os níveis de risco (impacto e probabilidade)
Encontrar novos controlos
Calcular o risco residual.

Post-FRAAP:
- Relatório final com sumário executivo, resumo da reunião, identificação de controlos complementares.
- 1 a 2 semanas.

Slide 5:

Business impact analysis (BIA):
- Se falhar um sistema de informação crítico, que efeitos isso vai ter na operação e viabilidade dos processos core de negócio.
- Para isso é preciso saber quais são os processos core.
- Quais os recursos utilizados pelos processos
- Classificar esses recursos.
- Requisitos para recuperação
- É importante os resultados para os Planos de continuidade de negócio

GAP analysis:
- Comparação entre o estado presente o estado que se quer (futuro)

- É preciso saber o estado atual, o que se quer atingir, e o que precisa de ser feito. (ISO27002)

Definir uma política de segurança:
- A política deve ser desdobrada em documentos auxiliares, que devem ter princípios e orientações para grupos específicos.
- Documento com regras que devem ser seguidas.
- Políticas de backups, teletrabalho, fornecedores, controles criptográficos etc.
- Pode incluir os procedimentos

Ameaças de privacidade:
- aplicações web vulneráveis
- Remoção de dados pessoais de maneira incorreta
- Coletar dados desnecessários
- Comunicação de dados via canais não seguros

Vulnerabilidades de privacidade:
- Não utilização de cifras nas comunicações.

Risco de privacidade:
- Incumprimento com o RGPD
- Exposição de dados confidenciais.

Ameaças da cloud:
- Misconfiguration of cloud services,
- Unauthorized access
- Insecure APIs
- External sharing of data
- Denial of service

Vulnerabilidades da cloud:
-