UEZO
CENTRO UNIVERSITÁRIO
ESTADUAL DA ZONA OESTE

Segurança Estratégica da Informação
ISO 27001, 27002 e 27005
Segunda Aula: ISO 27002

Prof. Dr. Eng. Fred Sauer
fsauer@gmail.com
http://www.fredsauer.com.br

ISO 27002 (17799) – Boas Práticas

- Objetivos de Controles e Controles
- Fazem parte do processo de SGSI
- Não exaustiva

Estabelecendo Requisitos de SegInfo

- Fontes
  - Análise/Avaliação do Risco → Identificação de ameaças. Vulnerabilidades e Impactos
  - Legislação que a corporação, parceiros, clientes e provedores tem que cumprir, bem como a cultura
  - Requisitos do Negócio

Análise/Avaliação de Riscos

- Gastos com controles devem ser balanceados com os danos causados ao negócio pelos incidentes de segurança
- Repetição periódica
- Controles devem ser escolhidos visando reduzir o risco a um patamar aceitável

Controles Essenciais (ponto de vista legal)

- Proteção de Dados e Privacidade das Informações pessoais
- Proteção dos Registros Organizacionais
- Direitos de Propriedade Intelectual

Controles considerados Práticas para SegInfo

- Documento da Política de SegInfo
- Atribuição de Responsabilidades
- Conscientização, educação e treinamento
- Processamento Correto das Aplicações
- Gestão de Vulnerabilidades Técnicas
- Gestão da Continuidade do Negócio
- Gestão de Incidentes e Melhorias

Obs.: Esta seleção é considerada um bom ponto de partida, mas NÃO substitui a seleção de controles com base na Análise de Riscos

Fatores Críticos de Sucesso

- PolSeg, objetivos e atividades que REFLITAM os objetivos do Negócio
- Uma abordagem e uma estrutura para o PDCA da SegInfo CONSISTENTE com a cultura
- COMPROMETIMENTO dos níveis Gerenciais
- ENTENDIMENTO dos Requisitos de SegInfo e do processo de Gestão de Riscos
- DIVULGAÇÃO eficiente da SegInfo
- DISTRIBUIÇÃO de Diretrizes e Normas da Política

Fatores Críticos de Sucesso (cont)

- PROVISÃO de Recursos Financeiros para a SegInfo
- CONSCIENTIZAÇÃO, EDUCAÇÃO e TREINAMENTO
- ESTABELECIMENTO da Gestão de Incidentes
- IMPLEMENTAÇÃO de um sistema de medição

Obs.: As métricas para o sistema de medição não fazem parte da norma 27002

Objetivos de Controle e Controles

- Política de Segurança
  - Política de Segurança da Informação – ***Objetivo***: orientar e apoiar, alinhado com o negócio e legislação
    - Documento Formal – ***Controle***: aprovado pela direção, publicado e comunicado a todos os interessados (internos e externos)
    - Análise Crítica da PolSeg – ***Controle***: análise regular ou em caso de mudanças, para assegurar pertinência, adequação e eficácia

Objetivos de Controle e Controles

- Organizando a SegInfo
  - Infraestrutura da SegInfo – ***Objetivo***: Gerenciar a SegInfo dentro da organização
    - Comprometimento da Direção – ***Controle***: Apoio da Direção através de claro direcionamento, atribuições e responsabilidades
    - Coordenação – ***Controle***: Representantes de diversas partes da organização com papéis relevantes
    - Responsabilidades – ***Controle***: Definição clara de responsabilidades
    - Processo de autorização – ***Controle***: Definição e implementação de um processo de gestão de autorização para novos recursos de processamento de informação
    - Acordos de Confidencialidade – ***Controle***: Refletir necessidades para a proteção da informação, com análise crítica regular

Objetivos de Controle e Controles

- Organizando a SegInfo (continuação)
  - Infra-estrutura da SegInfo – ***Objetivo***: Gerenciar a SegInfo dentro da organização
    - Contato com Autoridades – ***Controle***: Manutenção de contatos apropriados
    - Contato com Grupos Especiais – ***Controle***: Fóruns de Segurança e Associações Profissionais
    - Análise Crítica independente da SegInfo – ***Controle***: Realizada de forma independente. Periódica ou quando ocorrerem mudanças

Objetivos de Controle e Controles

- Organizando a SegInfo (continuação)
  - Partes Externas – ***Objetivo***: Manter a SegInfo quando há acesso, processamento, comunicação ou gerência externa
    - Identificação dos Riscos – ***Controle***: Os riscos e controles apropriados devem ser implementados antes de se conceder o acesso
    - Identificação da SegInfo no relacionamento com o Cliente – ***Controle***: Os requisitos de SegInfo para este segmento devem ser considerados antes de se conceder o acesso aos ativos ou informações da organização
    - Identificação da SegInfo nos acordos com terceiros – ***Controle***: Os acordos com terceiros devem cobrir todos os requisitos de SegInfo relevantes

Objetivos de Controle e Controles

- Gestão de Ativos
  - Responsabilidade pelos Ativos – ***Objetivo***: Alcançar e manter a proteção adequada dos ativos da organização
    - Inventário dos Ativos – ***Controle***: Inventário com clara identificação deve ser estruturado e mantido
    - Proprietário dos Ativos – ***Controle***: Associação dos recursos de processamento da informação com um responsável (pessoa ou organismo)
    - Uso Aceitável dos Ativos – ***Controle***: Regras para o uso das informações e de ativos

Objetivos de Controle e Controles

- Gestão de Ativos (continuação)
  - Classificação da Informação – ***Objetivo***: Assegurar que a informação tenha um nível adequado de proteção
    - Recomendações para Classificação – ***Controle***: A informação deve ser classificada segundo seu valor, requisitos legais, sensibilidade[1] e criticidade[2]
    - Rótulos e Tratamento da Informação – ***Controle***: Procedimentos para rotular e tratar a informação devem ser definidos de acordo com a classificação adotada

1 – Sensibilidade – suscetibilidade aos respectivos atributos

2 – Criticidade – grau subjetivo de importância para a continuidade do negócio

Objetivos de Controle e Controles

- Segurança em Recursos Humanos
  - Antes da Contratação[3] – ***Objetivo***: Assegurar que todos entendam suas responsabilidades e estejam de acordo com papéis definidos, reduzindo risco de roubo, fraude ou mau uso de recursos
    - Papéis e Responsabilidades – ***Controle***: definir e documentar o papel de todos na organização, fornecedores e terceiros, de acordo com a Política de SegInfo
    - Seleção – ***Controle***: Realizar verificações legais, regulamentares e éticas do elemento humano, proporcionais aos requisitos do negócio, classificação das informações e riscos
    - Termos e Condições de Contratação – ***Controle***: Todos devem concordar e assinar Termos e condições que declarem claramente as suas responsabilidades e da organização para preservação da SegInfo

3 – Contratação: contratação, nomeação, mudança de função ou cargo, contratos e etc.

Objetivos de Controle e Controles

- Segurança em Recursos Humanos (continuação)
  - Durante a Contratação – ***Objetivo***: Assegurar que todos estejam permanentemente conscientes dos aspectos de SegInfo, estando assim aptos a apoiar a política de SegInfo e reduzir riscos
    - Responsabilidades da Direção – ***Controle***: A Direção deve solicitar a todos que pratiquem a SegInfo de acordo com a Política
    - Conscientização, educação e treinamento em SegInfo – ***Controle***: Treinamento e atualizações regulares para todos, de acordo com suas funções e papéis
    - Processo Disciplinar – ***Controle***: Deve existir um processo disciplinar formal para os funcionários que cometam violações da SegInfo

Objetivos de Controle e Controles

- Segurança em Recursos Humanos (continuação)
  - Encerramento ou Mudança da Contratação – ***Objetivo***: Assegurar que todos que deixam o vínculo com a organização o façam de forma ordenada
    - Encerramento de Atividades – ***Controle***: As atividades necessárias para o encerramento ou a mudança de um trabalho devem ser claramente definidas e atribuídas
    - Devolução de ativos – ***Controle***: Um procedimento para devolução de ativos deve ser definido
    - Retirada de Direitos de Acesso – ***Controle***: Um procedimento para retirada ou alteração de direitos deve ser definido

Objetivos de Controle e Controles

- Segurança Física e do Ambiente
  - Áreas Seguras – *Objetivo*: Prevenir acesso físico não-autorizado
    - Perímetro de Segurança física – ***Controle***: Implementar barreiras (paredes, portões, recepcionistas, etc.) nas áreas que contenham informações e recursos de processamento de informações
    - Controles de Entrada Física – ***Controle***: Discriminar o acesso apenas ao pessoal autorizado
    - Segurança em Escritórios, salas e Instalações – ***Controle***: Projetar e aplicar recursos de acordo com a área
    - Proteção contra Ameaças Externas e do Meio Ambiente – ***Controle***: Proteções físicas contra incêndio, enchentes e outros desastres naturais ou causados pelo homem
    - Trabalhando em Áreas Seguras – ***Controle***: Procedimentos para o trabalho dentro dos Perímetros de Segurança
    - Acesso ao Público, Áreas de Entrega e Carregamento – ***Controle***: Implementar controle específico para estas áreas, de forma que se evite o acesso não-autorizado

Objetivos de Controle e Controles

- Segurança Física e do Ambiente (continuação)
  - Segurança de Equipamentos – ***Objetivo***: Impedir perdas, danos, furto ou comprometimento de ativos e interrupção das atividades da organização
    - Instalação e Proteção do Equipamento – ***Controle***: Procedimentos para alocação em ambiente seguro, reduzindo riscos de ameaças
    - Utilidades – ***Controle***: Proteção contra falta de energia elétrica e outras utilidades
    - Segurança no Cabeamento – ***Controle***: Proteção contra interceptação ou danos no cabeamento de energia e telecom que dá suporte aos serviços de informações
    - Manutenção dos Equipamentos – ***Controle***: Procedimentos para assegurar Disponibilidade e Integridade
    - Segurança de Equipamentos fora da Organização – ***Controle***: Procedimentos compatíveis com os riscos da operação fora dos perímetros internos da organização
    - Reutilização e alienação segura de equipamentos – ***Controle***: Assegurar que o descarte seja realizado adequadamente
    - Remoção de propriedade – ***Controle***: Ativos da Informação não devem ser retirados de seus locais sem autorização e providências peculiares

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações
  - Procedimentos e Responsabilidades operacionais – ***Objetivo***: Garantir a operação correta dos recursos de processamento da informação
    - Documentação dos Procedimentos de Operação – ***Controle***: Documentar, atualizar e disponibilizar toda documentação necessária para operar recursos da informação
    - Gestão de Mudanças – ***Controle***: Controlar modificações nos recursos de processamento de informações
    - Segregação de funções – ***Controle***: Compartimentar recursos para reduzir oportunidades de violação da SegInfo
    - Separação dos Recursos de Desenvolvimento, teste e Produção – ***Controle***: Garantir a separação para reduzir o risco de violações da Seginfo

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações (continuação)
  - Gerenciamento de Serviços Terceirizados – ***Objetivo***: Implementar o nível de SegInfo e garantir o cumprimento dos acordos de entrega de serviços
    - Entrega de serviços – ***Controle***: Procedimentos para garantir que os acordos de entrega sejam cumpridos (definições de serviços e controles de segurança)
    - Monitoramento e Análise Crítica de serviços Terceirizados – ***Controle***: Serviços, relatórios e registros fornecidos por terceiros devem ser regularmente auditados e analisados criticamente
    - Gerenciamento de Mudanças para Serviços Terceirizados – ***Controle***: Mudanças no contrato devem ser avaliadas e realizada a reanálise/reavaliação de riscos

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações (continuação)
  - Planejamento e Aceitação de Sistemas – ***Objetivo***: Minimizar o risco de falhas em sistemas
    - Gestão de Capacidade – ***Controle***: monitorar a utilização dos recursos e realizar projeções para necessidades de capacidade futura, visando garantir desempenho
    - Aceitação de Sistemas – ***Controle***: critérios para aceitação de novos sistemas, atualizações e novas versões, com testes durante o desenvolvimento e antes da aceitação

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações (continuação)
  - Proteção contra códigos maliciosos e códigos móveis – ***Objetivo***: Proteger a integridade do software e da informação
    - Controle contra códigos maliciosos – ***Controle***: implementação de controles de detecção, prevenção e recuperação, bem como conscientizar os usuários
    - Controle contra códigos móveis – ***Controle***: Deve ser definido uma configuração que códigos móveis não-autorizados não sejam executados e que os autorizados operem segundo uma política de seginfo

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações (continuação)
  - Cópias de Segurança – ***Objetivo***: Manter a Integridade e a Disponibilidade da Informação e dos recursos de processamento da informação
    - Cópias de segurança das Informações – ***Controle***: cópias das informações e softwares devem ser efetuadas e testadas regularmente, de acordo com uma política

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações (continuação)
  - Gerenciamento da Segurança em Redes – ***Objetivo***: Garantir a proteção das informações em redes e a proteção da infraestrutura de suporte
    - Controle das Redes – ***Controle***: Gerenciar e controlar as redes para proteger informações e sistemas que usam estas redes
    - Segurança dos Serviços de Redes – ***Controle***: Definição de aspectos de SegInfo peculiares às redes para inclusão nos acordos de serviços de rede, tanto internamente como para terceirizados

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações (continuação)
  - Manuseio de Mídias – ***Objetivo***: Prevenir divulgação não-autorizada, modificação, remoção ou destruição de ativos e interrupções das atividades do negócio
    - Gerenciamento de mídias removíveis – ***Controle***: Procedimentos para o gerenciamento
    - Descarte das Mídias – ***Controle***: Procedimentos formais de descarte
    - Procedimentos para o tratamento da informação – **Controle**: Procedimentos para o tratamento e armazenamento de informações, para evitar divulgação não-autorizada ou uso indevido
    - Segurança da Documentação dos Sistemas – **Controle**: A documentação deve ser protegida contra acessos não-autorizados

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações (continuação)
  - Troca de Informações – ***Objetivo***: Manter a SegInfo nas trocas de Informações internas e externas
    - Políticas e procedimentos para troca de informações – ***Controle***: Políticas e procedimentos devem ser formalizados para proteger informações em trânsito
    - Acordos para Troca de Informações – ***Controle***: Procedimentos bem definidos para trocas entre a organização e entidades externas
    - Mídias em trânsito – ***Controle***: Mídias contendo informações devem ser protegidas contra o acesso não autorizado, uso impróprio ou alteração indevida durante o transporte externo aos limites físicos da organização

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações (continuação)
  - Trocas de Informações (continuação)
    - Mensagens eletrônicas – ***Controle***: As informações que trafegam em mensagens eletrônicas devem ser adequadamente protegidas
    - Sistemas de informações do negócio – ***Controle***: Políticas e procedimentos devem ser desenvolvidos e implementados para proteger as informações associadas com a interconexão de sistemas de informações do negócio

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações (continuação)
  - Serviços de Comércio Eletrônico – ***Objetivo***: Garantir a Segurança de serviços de Comércio eletrônico e sua utilização segura
    - Comércio Eletrônico – ***Controle***: As informações envolvidas em comércio eletrônico transitando sobre redes públicas devem ser protegidas de atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas.
    - Transações on-line – ***Controle***: Informações envolvidas em transações *on-line* devem ser protegidas para prevenir transmissões incompletas, erros de roteamento, alterações não autorizadas de mensagens, divulgação não autorizada, duplicação ou reapresentação de mensagem não autorizada.
    - Informações publicamente disponíveis – ***Controle***: a Integridade das informações disponibilizadas em sistemas publicamente acessíveis deve ser protegida, para prevenir modificações não autorizadas

Objetivos de Controle e Controles

- Gerenciamento das Operações e Comunicações (continuação)
  - Monitoramento – ***Objetivo***: Detectar atividades não autorizadas de processamento de informação
    - Registros de Auditoria – ***Controle***: logs devem ser mantidos por um período acordado
    - Monitoramento do uso do Sistema – ***Controle***: Com procedimentos estabelecidos e análise crítica regular
    - Proteção dos Logs – ***Controle***: proteção contra falsificação e acesso não autorizado
    - Logs de administrador e Operador – ***Controle***: Registro específico destas atividades
    - Logs de Falhas – ***Controle***: Registro, análise e ações
    - Sincronização dos Relógios – ***Controle***: Todos os sistemas relevantes, de acordo com uma hora oficial

Objetivos de Controle e Controles

- Controle de Acessos
  - Requisitos de Negócio para Controle de Acesso – ***Objetivo***: Controlar o Acesso à Informação
    - Política de Controle de Acesso – ***Controle***: política estabelecida, documentada e analisada criticamente com base nos requisitos do negócio

Objetivos de Controle e Controles

- Controle de Acessos (continuação)
  - Gerenciamento de Acesso do Usuário – ***Objetivo***: Assegurar acesso ao usuário autorizado e prevenir o acesso não autorizado
    - Registro de Usuário – ***Controle***: Registro e Cancelamento formalizados com garantias de revogação de direitos
    - Gerenciamento de Privilégios – ***Controle***: Concessão e uso restritos e controlados
    - Gerenciamento de Senhas – ***Controle***: Processo de concessão e gerenciamento formalizado
    - Análise Crítica de Direitos de Acesso – ***Controle***: Análise Crítica regular formalizada

Objetivos de Controle e Controles

- Controle de Acessos (continuação)
  - Responsabilidades dos Usuários – ***Objetivo***: Prevenir acesso não autorizado e evitar o comprometimento ou roubo da informação e seus recursos
    - Uso de senhas – ***Controle***: orientação para a seleção e o uso de boas práticas
    - Equipamento de Usuário sem monitoração – ***Controle***: proteção adequada para equipamentos não monitorados
    - Política de Mesa Limpa e Tela Limpa – ***Controle***: mesa limpa de papéis e mídias e tela limpa de informações

Objetivos de Controle e Controles

- Controle de Acessos (continuação)
  - Controle de Acesso à Rede – ***Objetivo***: Prevenir o acesso não autorizado
    - Política de Uso dos Serviços – ***Controle***: Acesso apenas aos serviços com específica autorização
    - Autenticação para Conexão Externa – ***Controle***: Métodos apropriados de autenticação
    - Identificação de Equipamento em Rede – ***Controle***: Identificações automáticas de acordo com localização e equipamentos específicos
    - Proteção e Configuração de Portas de Diagnóstico Remotas – ***Controle***: Controle físico e lógico destas portas
    - Segregação de Redes – ***Controle***: Segregação por Grupos de Serviços, Usuários e Sistemas
    - Controle de Conexão de Rede – ***Controle***: Restrição da capacidade de Conexão de acordo com a Política
    - Controle de Roteamento – ***Controle***: Assegurar a não violação da Polseg para computadores e fluxos de informação

Objetivos de Controle e Controles

- Controle de Acessos (continuação)
  - Controle do Acesso ao Sistema Operacional – ***Objetivo***: Prevenir acesso não autorizado
    - Procedimentos de log-on – ***Controle***: Acesso aos SO controlado por um procedimento seguro
    - Identificação e Autenticação de Usuário – ***Controle***: Todos usuários com ID única para uso pessoal e exclusivo, com técnica de autenticação para validação da identidade alegada
    - Sistema de Gerenciamento de Senhas – ***Controle***: Interativos e asseguradores de senhas de qualidade
    - Uso de Utilitários com Capacidade de Sobrepor Controles de Acesso – ***Controle***: Restritos e estritamente controlados
    - Desconexão por Inatividade – ***Controle***: Desconexão após um período definido de inatividade
    - Limitação de Horário de Conexão – ***Controle***: Restrições para acesso por horários

Objetivos de Controle e Controles

- Controle de Acessos (continuação)
  - Controle do Acesso à Aplicação e à Informação – ***Objetivo***: Prevenir acesso à informação contida nos sistemas
    - Restrição de Acesso à Informação – ***Controle***: Restrição de acesso aos usuários e ao pessoal de suporte à informação e funcionalidades de sistemas de acordo com a Polseg
    - Isolamento de Sistemas Sensíveis – ***Controle***: Isolamento em ambiente computacional dedicado

Objetivos de Controle e Controles

- Controle de Acessos (continuação)
  - Computação Móvel e Trabalho Remoto – ***Objetivo***: Garantia da Segurança
    - Computação e Comunicação Móvel – ***Controle***: Formalização de uma Política específica para proteção contra os riscos nestes acessos
    - Trabalho Remoto – ***Controle***: Desenvolvimento e implementação de uma política e planos operacionais para o trabalho remoto

Objetivos de Controle e Controles

- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação
  - Requisitos de Segurança de Sistemas de Informação – ***Objetivo***: Garantir a integração da segurança em Sistemas de Informação
    - Análise e Especificação de Requisitos de Segurança – ***Controle***: Novos Sistemas ou melhorias em Sistemas existentes com controles de segurança

Objetivos de Controle e Controles

- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (continuação)
  - Processamento correto de aplicações – ***Objetivo***: Prevenir ocorrência de erros, perdas, modificação não autorizada ou mau uso das informações
    - Validação de Dados de Entrada – ***Controle***: Garantia de dados corretos e apropriados
    - Controle do Processamento Interno – ***Controle***: checagens para detecção de informações corrompidas
    - Integridade de mensagens – ***Controle***: Garantia da Autenticidade e Integridade de mensagens em aplicações
    - Validação de Dados de Saída – Controle: ***Garantia*** de dados corretos e apropriados

Objetivos de Controle e Controles

- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (continuação)
  - Controles Criptográficos – ***Objetivo***: Proteger a Confidencialidade, a Autenticidade ou a Integridade
    - Política de uso de controles criptográficos – ***Controle***: Desenvolver e implementar uma política de uso de controles criptográficos
    - Gerenciamento de Chaves – ***Controle***: Implantação de um processo de gerenciamento de chaves para apoio de técnicas criptográficas

Objetivos de Controle e Controles

- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (continuação)
  - Segurança dos Arquivos do Sistema – ***Objetivo***: Garantir a Segurança de Arquivos do Sistema
    - Controle de Software Operacional – ***Controle***: Procedimentos para instalação de SO
    - Proteção de Dados para Teste de Sistema – ***Controle***: Seleção cuidadosa, proteção e controle de dados para testes
    - Controle de Acesso ao Código-fonte de Programas – ***Controle***: Restrição de acesso

Objetivos de Controle e Controles

- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (continuação)
  - Segurança em Processos de Desenvolvimento e de Suporte – ***Objetivo***: Manter a Segurança de Aplicativos e da Informação
    - Procedimentos para Controle de Mudanças – ***Controle***: Procedimentos formais
    - Análise Crítica Técnica das aplicações após mudanças no SO – ***Controle***: Garantias de não haver impacto na operação ou na segurança
    - Restrições sobre Mudanças em Pacotes de Software – ***Controle***: limitar apenas às mudanças necessárias, que devem ser feitas sob controle
    - Vazamento de Informações – ***Controle***: Prevenção de oportunidades
    - Desenvolvimento Terceirizado de Software – ***Controle***: Supervisionar e monitorar o desenvolvimento terceirizado

Objetivos de Controle e Controles

- Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação (continuação)
  - Gestão de Vulnerabilidades Técnicas – ***Objetivo***: Reduzir Riscos Resultantes da Exploração de Vulnerabilidades Técnicas Conhecidas
    - Controle de Vulnerabilidades Técnicas – ***Controle***: Obtenção da informação sobre a existência de vulnerabilidades nos sistemas em uso, avaliação da exposição e medidas para lidar com os riscos associados

Objetivos de Controle e Controles

- Gestão de Incidentes de Segurança da Informação
  - Notificação de Fragilidades e Eventos de Segurança da Informação – ***Objetivo***: Assegurar que fragilidades e eventos de SegInfo sejam comunicados, visando a ação corretiva em tempo hábil
    - Notificação de Eventos de SegInfo – ***Controle***: Uso de canais apropriados para relato de eventos à Direção o mais rapidamente possível
    - Notificação de Fragilidades de SegInfo – ***Controle***: Instruir funcionários, fornecedores e parceiros a registrar e notificar qualquer observação ou suspeita em sistemas ou serviços

Objetivos de Controle e Controles

- Gestão de Incidentes de Segurança da Informação (continuação)
  - Gestão de Incidentes de Segurança da Informação e melhorias – ***Objetivo***: Assegurar um enfoque consistente e efetivo
    - Responsabilidades e Procedimentos – ***Controle***: Estabelecimento para assegurar respostas rápidas, efetivas e ordenadas
    - Aprendendo com os Incidentes – ***Controle***: mecanismos de monitoramento e quantificação de tipos e quantidades de incidentes
    - Coleta de Evidências – ***Controle***: Coleta, armazenamento e apresentação de evidências contra uma pessoa ou organização, após um incidente que envolva ação legal (civil ou criminal), de acordo com normas da jurisdição

Objetivos de Controle e Controles

- Gestão da Continuidade do Negócio
  - Aspectos da Gestão da Continuidade do Negócio, relativos à SegInfo – ***Objetivo***: Não permitir a interrupção das atividades do negócio, proteger os processos críticos contra efeitos de falhas ou desastres e assegurar sua retomada em tempo hábil
    - Incluindo a SegInfo no processo de Gestão da Continuidade do Negócio – ***Controle***: Contemplação dos requisitos de SegInfo no processo de Gestão da continuidade do Negócio
    - Continuidade de Negócios e Análise/Avaliação de Risco – ***Controle***: Identificação de eventos que podem causar interrupção nos Processos de Negócio, junto à probabilidade de impacto e suas consequências
    - Desenvolvimento e implantação de Planos de Continuidade relativos à SegInfo – ***Controle***: Planos para Manutenção ou recuperação das operações no tempo e nível requeridos
    - Estrutura do Plano de Continuidade dos Negócios – ***Controle***: Manter uma estrutura para assegurar consistência, contemplação de requisitos e identificação de prioridades para testes e manutenção
    - Testes, Manutenção e Reavaliação dos PCN – ***Controle***: Testes e atualização regulares, para assegurar atualização e efetividade

Objetivos de Controle e Controles

- Conformidade
  - Conformidade com Requisitos Legais – ***Objetivo***: Evitar violação de qualquer requisito legal
    - Identificação da Legislação Vigente – ***Controle***: Requisitos estatutários, regulamentares e contratuais e o enfoque da organização para seu atendimento devem estar documentados e atualizados
    - Direitos de Propriedade Intelectual – ***Controle***: Procedimentos para sua garantia
    - Proteção de Registros Organizacionais – ***Controle***: Proteção contra perda, destruição e falsificação de acordo com regulamentos, estatutos, contratos e requisitos do negócio
    - Proteção de Dados e Privacidade da Informação pessoal – ***Controle***: Assegurar a proteção de dados e privacidade de acordo com a legislação e clausulas contratuais
    - Prevenção contra Mau Uso – ***Controle***: Dissuasão do mau uso dos recursos do processamento da Informação para propósitos não autorizados
    - Regulamentação de Controles de Criptografia – ***Controle***: Uso de acordo com a legislação, acordos e regulamentações

Objetivos de Controle e Controles

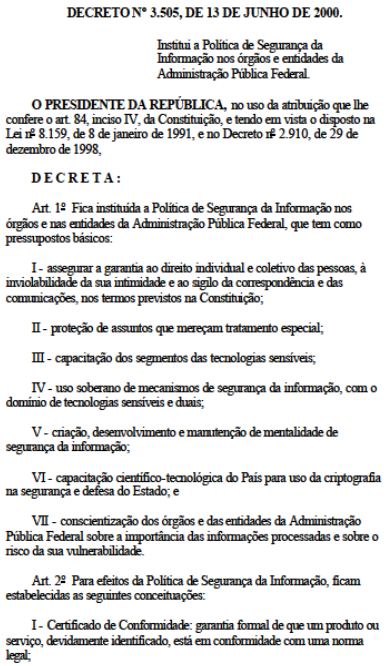
- Conformidade (continuação)
  - Conformidade com Normas e Políticas de SegInfo e Conformidade Técnica – ***Objetivo***: Garantir conformidade dos Sistemas com as Políticas e Normas Organizacionais
    - Conformidade com as Políticas e Normas da SegInfo – ***Controle***: Os gestores devem garantir que os procedimentos em suas áreas de responsabilidade sejam cumpridos
    - Verificação de Conformidade Técnica – ***Controle***: Verificação periódica de conformidade

Objetivos de Controle e Controles

- Conformidade (continuação)
  - Considerações quanto à Auditoria de Sistemas – ***Objetivo***: Maximizar a Eficácia e Minimizar a Interferência no Processo de Auditoria
    - Controles de Auditoria de Sistemas de Informação – ***Controle***: Os requisitos e atividades de auditoria devem ser planejados e acordados para minimizar riscos de interrupção nos Processos de Negócio
    - Proteção de Ferramentas de Auditoria de Sistemas de Informação – ***Controle***: As ferramentas devem ser protegidas para evitar uso impróprio ou comprometimento

Política de Segurança - Exemplo

- DL 3505/2000 – PS do Governo Federal – foco em Diretrizes
- Destaques:
  - Simples, estabelece 8 objetivos e 14 diretrizes
  - Dá competência a ABIN/CEPESQ para a condução do processo
  - Criação CGSI sob coordenação do GSIPR



DECRETO Nº 3.505, DE 13 DE JUNHO DE 2000.

Institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal.

O PRESIDENTE DA REPÚBLICA, no uso da atribuição que lhe confere o art. 84, inciso IV, da Constituição, e tendo em vista o disposto na Lei nº 8.159, de 8 de janeiro de 1991, e no Decreto nº 2.910, de 29 de dezembro de 1998,

D E C R E T A :

Art. 1º Fica instituída a Política de Segurança da Informação nos órgãos e nas entidades da Administração Pública Federal, que tem como pressupostos básicos:

I - assegurar a garantia ao direito individual e coletivo das pessoas, à inviolabilidade da sua intimidade e ao sigilo da correspondência e das comunicações, nos termos previstos na Constituição;

II - proteção de assuntos que mereçam tratamento especial;

III - capacitação dos segmentos das tecnologias sensíveis;

IV - uso soberano de mecanismos de segurança da informação, com o domínio de tecnologias sensíveis e duais;

V - criação, desenvolvimento e manutenção de mentalidade de segurança da informação;

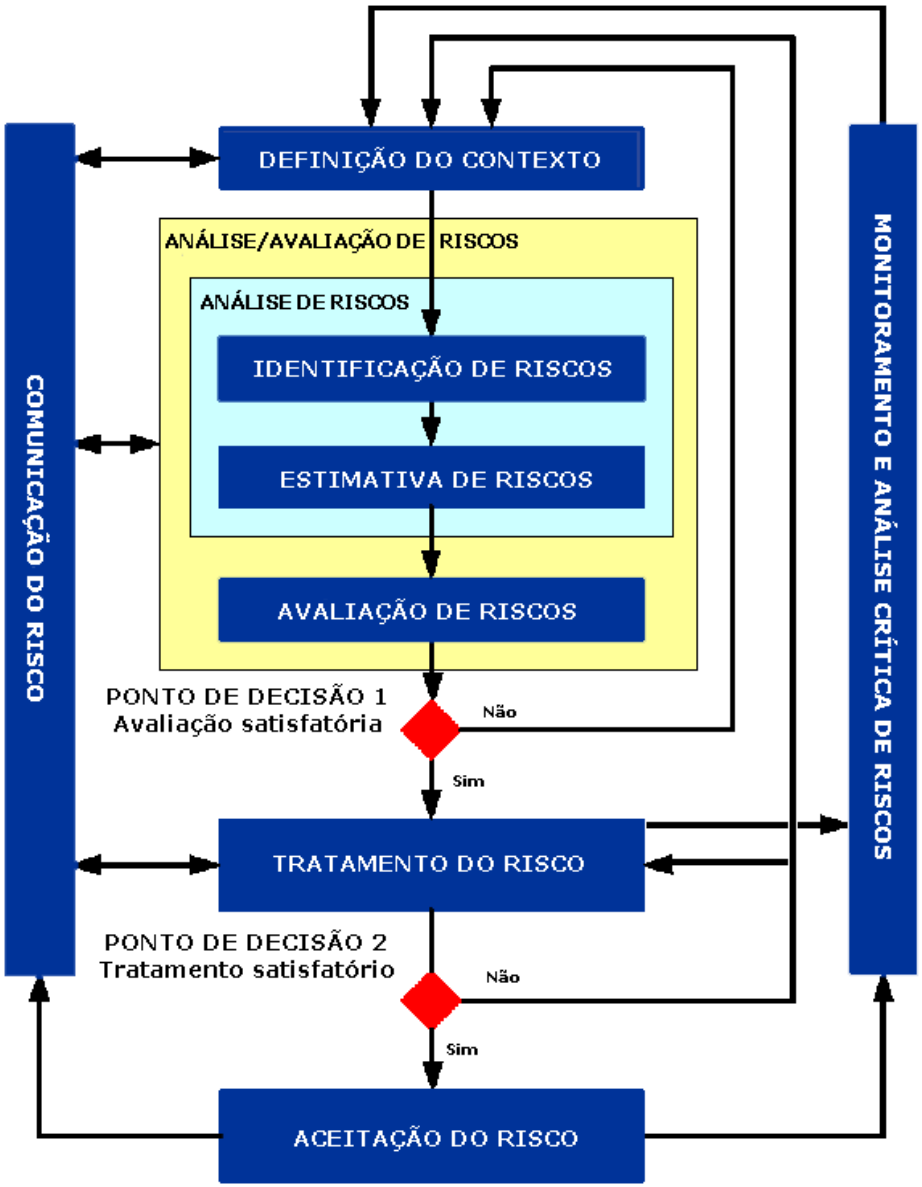
VI - capacitação científico-tecnológica do País para uso da criptografia na segurança e defesa do Estado; e

VII - conscientização dos órgãos e das entidades da Administração Pública Federal sobre a importância das informações processadas e sobre o risco da sua vulnerabilidade.

Art. 2º Para efeitos da Política de Segurança da Informação, ficam estabelecidas as seguintes conceituações:

I - Certificado de Conformidade: garantia formal de que um produto ou serviço, devidamente identificado, está em conformidade com uma norma legal;

ISO 27005:2008



FIM DA PRIMEIRA OU DAS DEMAIS INTERAÇÕES