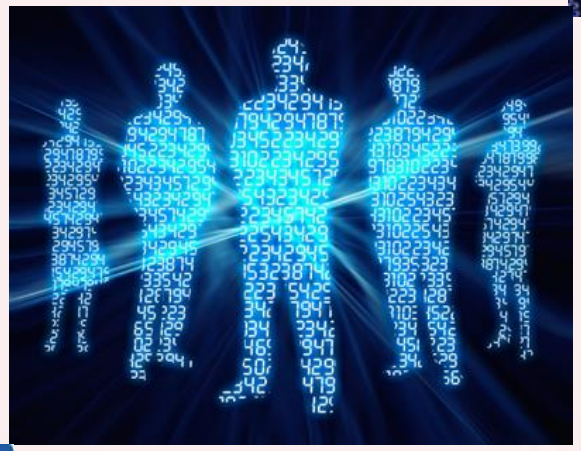
Treinamento Básico em Segurança da Informação



ISO 27001 ISMS

information security
ISO/IEC 2702

Módulo 1

Visão geral das normas

NBR ISO/IEC 27001 , ISO/IEC 27002 e demais

Normas Base para a Legislação em S.I. no Brasil

Treinamento Básico em Segurança da Informação

A ISO “International Organization forStandardization” é uma organização sediada em Genebra, na Suiça. Foi fundada em 1946.

A sigla ISO foi originada da palavra isonomia.

O propósito da ISO é desenvolver e promover normas que possam ser utilizadas igualmente por todos os países do mundo.

Uma rede de institutos de normas nacionais de 162 países integram esta importante organização,

O Brasil é representado pela Associação Brasileira de Normas Técnicas - ABNT

ISO International Organization for Standardization

Treinamento Básico em Segurança da Informação

As duas normas principais relativas a Segurança da Informação são:

NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão da Segurança da Informação

NBR ISO/IEC 27002:20135 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para controles de segurança da informação

Treinamento Básico em Segurança da Informação

Outras normas da família ISO27000 importantes para a segurança da informação:

NBR ISO/IEC 27003:2011 – Tecnologia da Informação – Técnicas de Segurança – Diretrizes para implantação de um sistema de gestão da segurança da informação;

NBR ISO/IEC 27004:2017 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de gestão da segurança da informação – Monitoramento, medição, análise e avaliação;

NBR ISO/IEC 27005:2011 – Tecnologia da Informação – Técnicas de Segurança – Gestão de riscos de segurança da informação;

NBR ISO/IEC 27007:2012 – Diretrizes para auditoria de sistemas de gestão da segurança da informação;

NBR ISO/IEC 27014:2013 – Tecnologia da Informação – Técnicas de Segurança – Governança de segurança da informação

NBR ISO/IEC 27017:2016 – Tecnologia da Informação – Técnicas de Segurança – Código de prática para controles de segurança da informação com base ABNT NBR ISO/IEC 27002 para serviços em nuvem

NBR ISO/IEC 27037:2013 – Tecnologia da Informação – Técnicas de Segurança – Diretrizes para identificação, coleta, aquisição e preservação de evidência digital;

NBR ISO/IEC 27038:2014 – Tecnologia da Informação – Técnicas de Segurança – Especificação para redação digital

Treinamento Básico em Segurança da Informação

NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão da Segurança da Informação - Requisitos

- Primeira edição traduzida foi publicada em Outubro de 2005 e substituiu a norma BS 7799-2 para certificação de sistema de gestão de segurança da informação;

- É um padrão britânico que foi adotado pela ISO e trata da definição de requisitos para um Sistema de Gestão da Segurança da Informação.

- A norma identifica requisitos de controle que as organizações devem adotar, no entanto não necessariamente devendo restringir-se somente a eles.

- Esta norma é utilizada como guia para auditoria de certificação.

- Parte do sistema de gestão, baseado no enfoque de riscos inerentes aos ativos de informação, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação.

- Considera a segurança: física, técnica, procedimental e em pessoas

Treinamento Básico em Segurança da Informação

NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistema de Gestão da Segurança da Informação

- Incorpora um processo de inventário de ativos e dá uma ênfase a gestão de riscos
- Adota como os demais sistemas de gestão o ciclo PDCA e a versão 2013 estabelece uma maior aderência aos demais sistemas de gestão ;
- Dá um grande enfoque ao comprometimento da alta direção e no treina-mento dos funcionários
- Controles adicionais podem ser incorporados ao SGSI.

A norma ISO27003 estabelece como primeiro passo na implementação de um SGSI: obtendo a aprovação da direção para iniciar o projeto do SGSI.

Treinamento Básico em Segurança da Informação

NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistema de gestão da segurança da informação - Requisitos

Capítulos da Norma:

0. Introdução
1. Escopo;
2. Referências normativas;
3. Termos e definições;
4. Contexto da Organização
5. Liderança;
6. Planejamento;
7. Apoio;
8. Operação;
9. Avaliação de Desempenho;
10. Melhoria;

Anexo A

Treinamento Básico em Segurança da Informação

NBR ISO/IEC 27001:2013 – Tecnologia da Informação – Técnicas de Segurança – Sistema de gestão da segurança da informação - Requisitos

Controles do Anexo A da norma:

A5. Políticas de segurança da informação;
A6. Organização da segurança da informação;
A7. Segurança em recursos humanos;
A8. Gestão de ativos;
A9. Controle de acesso;
A10. Criptografia;
A11. Segurança física e do ambiente;
A12. Segurança nas operações;
A13. Segurança nas comunicações;
A14. Aquisição, desenvolvimento e manutenção de sistemas;
A15. Relacionamento na cadeia de suprimento;
A16. Gestão de incidentes de segurança da informação;
A17. Aspectos da segurança da informação na gestão de continuidade dos negócios;
A18. Conformidade

Treinamento Básico em Segurança da Informação

NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Gestão da Segurança da Informação

- Substituiu a Norma NBR ISO/IEC 27002:2005
- Consiste em 35 objetivos de controle e 114 controles
- Está estruturada em 11 capítulos
- Baseada nas melhores práticas em segurança da informaçã utilizada como documento de referência;
- Não pode ser utilizada em auditorias e certificações;

Treinamento Básico em Segurança da Informação

NBR ISO/IEC 27002:2013 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Gestão da Segurança da Informação

Capítulos da Norma:

0. Introdução
1. Escopo;
2. Referência normativa;
3. Termos e definições;
4. Estrutura desta norma;
5. Políticas de segurança da informação;
6. Organização da segurança da informação;
7. Segurança em recursos humanos;
8. Gestão de ativos;
9. Controle de acesso;
10. Criptografia;
11. Segurança física e do ambiente;
12. Segurança nas operações;
13. Segurança nas comunicações;
14. Aquisição, desenvolvimento e manutenção de sistemas;
15. Relacionamento na cadeia de suprimento;
16. Gestão de incidentes de segurança da informação;
17. Aspectos da segurança da informação na gestão da continuidade dos negócios;
18. Conformidade

Treinamento Básico em Segurança da Informação

Vantagens obtidas através da implementação de um Sistema de Gestão da Segurança da Informação segundo a norma ISO 27002 e certificado segundo a norma ISO 27001.

- Requisito fundamental para a Governança Corporativa e de TI;
- Melhoria da eficácia da Segurança da Informação;
- Diferencial competitivo;
- Normas de aceitação mundial;
- É garantia de continuidade operacional;
- Atende exigências normativas e de clientes.
- Compilação das melhores práticas;

Treinamento Básico em Segurança da Informação

ISO 27001 dados de 2018

A certificação ISO 27001 novamente aparece no topo da lista de crescimento e continuará crescendo devido as regulações internacionais de proteção de dados, como GDPR, LGPD e outras. China, Japão, Reino Unido e Índia figuram no topo da lista, como países com o maior número de empresas certificadas ISO 27001, tudo indica que nos próximos anos o Brasil fará parte dessa lista.

ISO 27701 Extensão da ISO27001 e 27002 – Sistemas de Gestão de Informação Privada, foi publicada no dia 05 de agosto de 2019 e tem como objetivo estabelecer controles de segurança para proteção de dados, sendo uma adequação lógica para LGPD e GDPR.

A ISO 27701 é um padrão internacional para proteção de dados, a Norma chega ao mercado para ser uma ferramenta internacional de adequação as mais diversas regulações de proteções de dados em diversos países, como a LGPD – Lei Geral de Proteção de Dados do Brasil e a GDPR – General Data Protection Regulation da Europa.

Treinamento Básico em Segurança da Informação

ISO 37001 dados 2018

Sobre a ISO 37001 é nítido que os países latinos, figuram com o maior número de certificações, como o Brasil, seguidos também por países orientais como Coréia do Sul e Malásia. Fato importante é que, o Reino Unido figura em posição de destaque na Europa e é também observado que começam as certificações de ISO 37001 nos Estados Unidos, países esses com grande cultura em **Compliance Antissuborno.** Pelo fato de ser uma norma recente e ter figurado com grande aceitação de grandes players globais na busca pela certificação e principalmente na exigência de certificação à alguns tipos específicos de fornecedores, é nítido que as empresas certificadas ISO 37001 irão ter forte crescimentos nos próximos anos.

FIM do Módulo 1

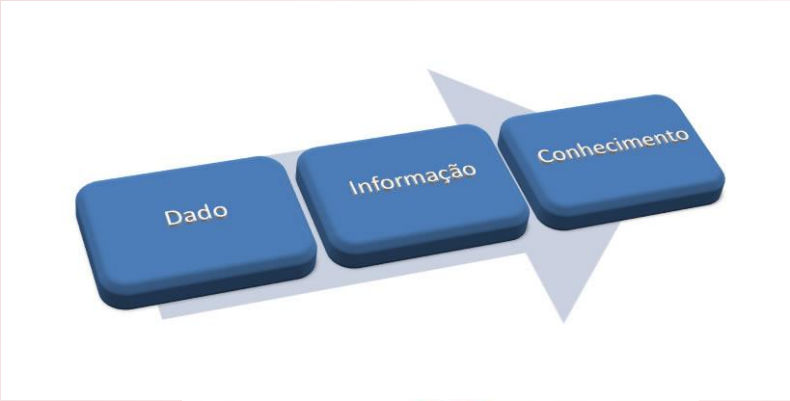
Visão geral das normas

NBR ISO/IEC 27001, ISO/IEC 27002 e Complementares

Módulo 2

Conceitos: Informação, ativos de informação, confidencialidade, disponibilidade, integridade, vulnerabilidades, ameaças, impactos, probabilidades

Treinamento Básico em Segurança da Informação



Dado de maneira geral, é o conteúdo quantificável e que por si só não transmite nenhuma mensagem que possibilite o entendimento sobre determinada situação. Os dados podem ser considerados a unidade básica da informação.

A **informação** é a ordenação e organização dos dados de forma a transmitir significado e compreensão dentro de um determinado contexto. Seria o conjunto ou consolidação dos dados de forma a fundamentar o **conhecimento**.

Treinamento Básico em Segurança da Informação

Ativos de Informação

O valor da **informação** vai além das palavras escritas, números e imagens: conhecimento, conceitos, ideias e marcas são exemplos de formas intangíveis da informação. Em um mundo interconectado, a informação e os processos relacionados, sistemas, redes e pessoas envolvidas nas suas operações são informações que, como outros **ativos** importantes, têm valor para o negócio da organização e, consequentemente, requerem proteção contra vários riscos.

Treinamento Básico em Segurança da Informação

Tipos de Informação

Impressa ou escrita em papel

Armazenada eletronicamente

Transmitida pelo correio ou
Meios eletrônicos.

Mostrada em vídeos

Verbal – falada em conversações

Não importa a forma que a informação toma ou os meios pelos quais ela é armazenada ou compartilhada. Ela deve ser sempre adequadamente protegida.

Tipos de informações a serem protegidas

INTERNAS – Aquela que não deve ser conhecida pelos concorrentes

DE CLIENTES OU FORNECEDORES – Informação que eles não querem que você divulgue.

DE PARCEIROS – Informação que necessita ser compartilhada entre parceiros comerciais

Segurança da Informação

Segundo a NBR ISO/IEC 27001

Segurança da Informação - é a preservação da confidencialidade, integridade e disponibilidade da informação; adicionalmente, outras propriedades tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também estar envolvidas.

Atributos/propriedades da Informação relativas à segurança

Segundo a NBR ISO/IEC 27001

Confidencialidade – propriedade de que a informação não esteja disponível ou revelada a indivíduos, entidades ou processos não autorizados;

Integridade – A integridade se refere a propriedade de estar correto e consistente com o estado ou a informação pretendida. Qualquer modificação não autorizada de dados, quer deliberada ou acidental, é uma violação da integridade dos dados.

Atributos/propriedades da Informação relativas à segurança

Segundo a NBR ISO/IEC 27001

Disponibilidade – propriedade de estar acessível e utilizável sob demanda por uma entidade autorizada.
As características de disponibilidade são:

- **Oportunidade:** a informação está disponível quando necessário
- **Continuidade:** a equipe consegue continuar trabalhando no caso de falha.
- **Robustez:** existe capacidade suficiente para permitir que não hajam interrupções ocasionadas pela insuficiência de recursos técnicos.

Atributos/propriedades da Informação relativas à segurança

Autenticidade – A autenticidade relaciona-se com a confirmação de autoria, a certificação e a originalidade da informação. Uma das formas para verificar a autenticidade em meio eletrônico é a assinatura digital.

Não-repúdio – Visa garantir que o autor não negue ter criado e assinado o documento.

Confiabilidade – é a capacidade do software manter seu nível de desempenho quando usado nas condições especificadas. Com eficácia em um nível de qualidade aceitável.

Treinamento Básico em Segurança da Informação

A segurança da informação objetiva a manutenção do equilíbrio entre os atributos da informação

DISPONIBILIDADE

CONFIDENCIALIDADE

INTEGRIDADE

CONFIABILIDADE

NÃO REPÚDIO

AUTENTICIDADE

Treinamento Básico em Segurança da Informação

“A Segurança da Informação é obtida a partir da implementação de uma série de controles, que podem ser políticas, práticas, procedimentos, estruturas organizacionais e funções de software. Estes controles precisam ser estabelecidos para garantir que os objetivos específicos da organização sejam atendidos” NBR ISO/IEC 27002

Treinamento Básico em Segurança da Informação

Vulnerabilidades são fraquezas associadas aos controles implementados quanto a segurança dos ativos de informação. A análise de vulnerabilidades tem por objetivo verificar a existência de falhas de segurança no ambiente de TIC das empresas. Esta análise é uma ferramenta importante para a implementação de controles de segurança eficientes sobre os ativos de informação das empresas.

Treinamento Básico em Segurança da Informação

A análise de vulnerabilidade sobre ativos da informação compreende Tecnologias, Processos, Pessoas e Ambientes;

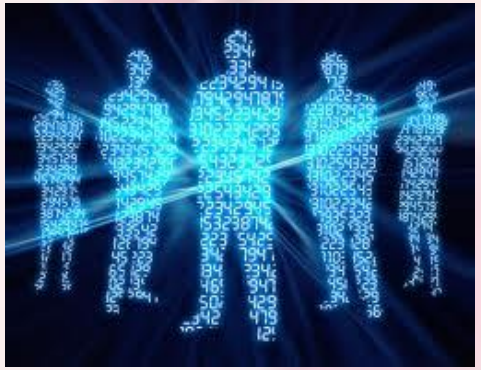
Tecnologias: software e hardware usados em servidores, estações de trabalho e outros equipamentos pertinentes, como sistemas de telefonia, rádio e gravadores; Ex.: estações sem anti-vírus, servidores sem detecção de intrusão, sistemas sem identificação ou autenticação;

Processos: análise do fluxo de informação, da geração da informação e de seu consumo. Analisa também como a informação é compartilha entre os setores da organização; Ex.: Em um processo de compra, se a lista de compra for passada de modo errôneo, esta pode ser deletada ou esquecida, ou interpretada errado. Causando a indisponibilidade do processo ou a falta de integridade dos resultados do processo.

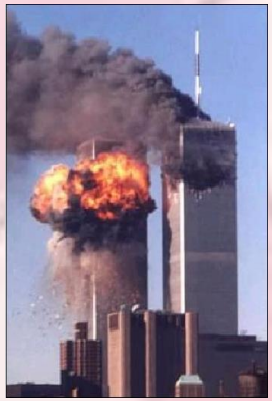
Pessoas: as pessoas são ativos da informação e executam processos, logo, precisam ser analisadas. Pessoas podem possuir importantes vulnerabilidades. Ex.: Desconhecer a importância da segurança, desconhecer suas obrigações e responsabilidades, deixando processos com “dois pais” e outros “órfãos”.

Ambientes: é o espaço físico onde acontecem os processos, onde as pessoas trabalham e onde estão instalados os componentes de tecnologia. Este item é responsável pela análise de áreas físicas. Ex.: Acesso não autorizado a servidores, arquivo e fichários;

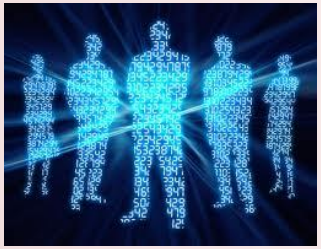
Treinamento Básico em Segurança da Informação



Ameaças são quaisquer circunstâncias ou eventos com o potencial de causar impacto negativo sobre a confidencialidade, integridade ou disponibilidade de informação ou sistemas de informação



Treinamento Básico em Segurança da Informação



Ameaças
Uma ameaça é um evento que acarreta algum perigo a um bem.
Evento é um fato causador de perda.

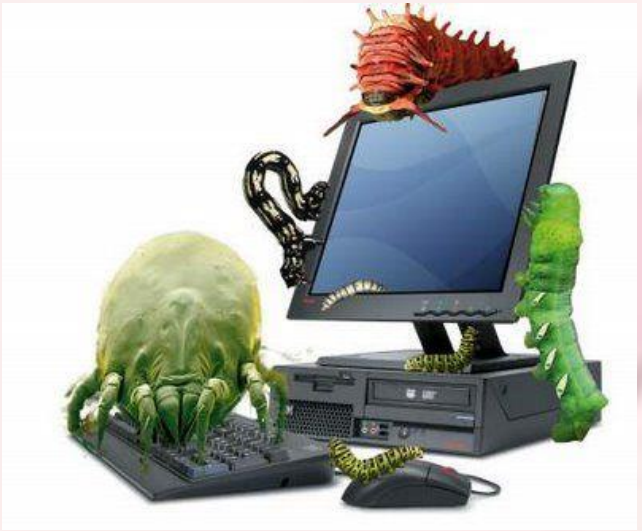
Agente da Ameaça
É uma entidade que pode iniciar a ocorrência de uma ameaça.
Entidade: uma pessoa: o invasor, o intruso

Ameaças Não Intencionais
Erros humanos,
Falhas em equipamentos,
Desastres naturais,
Problemas em comunicações.

Ameaças Intencionais
Roubo,
Vandalismo,
Utilização de recursos, violando as medidas de segurança
Ato de terrorismo

Treinamento Básico em Segurança da Informação

Probabilidade em Segurança da Informação é o grau de previsibilidade de uma ameaça explorar uma vulnerabilidade aproveitando-se de uma potencial ausência de controle. Exemplo: ausência de anti-virus possibilita a probabilidade de infecção por programas maliciosos.



Treinamento Básico em Segurança da Informação

Impacto em Segurança da Informação referem-se aos resultados indesejados da ação (ocorrência) de uma ameaça contra um bem, que resulta em perda mensurável para uma organização. Estes impactos podem ser financeiros, dano de imagem, perda da credibilidade, descontinuidade operacional, etc..

Fim do Módulo 2

Conceitos: Informação, ativos de informação, confidencialidade, disponibilidade, integridade, vulnerabilidades, ameaças, impactos, probabilidades

Módulo 3

Gestão de Riscos em Segurança da Informação

Análise avaliação e tratamento de Riscos.

Aceitação de Riscos

Treinamento Básico em Segurança da Informação

Ameaça

Uma ameaça é um evento indesejado em potencial. Quando uma ameaça se transforma num evento real temos um incidente indesejado que pode prejudicar um sistema ou uma organização.

Vulnerabilidade

Uma vulnerabilidade é uma fraqueza de um ativo ou controle que pode potencialmente ser explorado por uma ou mais ameaças.

Treinamento Básico em Segurança da Informação

Riscos em Segurança da Informação

Efeito da incerteza sobre os objetivos.

O risco em segurança da informação é frequentemente expresso como uma combinação de dois fatores: probabilidade e consequências. Ele faz duas perguntas básicas: Qual é a probabilidade de que um determinado evento de segurança da informação ocorra o futuro? E que consequências esse evento produziria ou o que impacto teria se realmente ocorresse?

Os riscos de segurança da informação geralmente surgem porque as ameaças de segurança em potencial identificadas exploram as vulnerabilidades de um ativo de informação ou grupo de ativos e, portanto, causam danos a uma organização.

Treinamento Básico em Segurança da Informação

Exemplos de Riscos em Segurança da Informação

Interrupção das operações da organização
Indisponibilidade de infromações críticas
Divulgação de dados incorretos
Perda ou roubo de ativos de informação
Abalos na credibilidade ou imagem por eventos de segurança
Divulgação indevida de dados confidenciais
Etc.

Treinamento Básico em Segurança da Informação

Gestão de Riscos em Segurança da Informação

O processo de Gestão de Riscos é a pedra fundamental de um Sistema de Gestão da Segurança da Informação. De tal forma a Gestão de Riscos afeta a Segurança da Informação que a ISO publicou uma norma específica para tal, a NBR ISO/IEC 27005 – Tecnologia da Informação – Técnicas de segurança – Gestão de riscos de segurança da informação.

Gestão de Riscos em Segurança da Informação

Convém que a gestão de riscos de segurança da informação seja um processo contínuo. Convém que o processo defina os contextos interno e externo, avalie os riscos e trate os riscos usando um plano de tratamento a fim de implementar as recomendações e decisões. Convém que a gestão de riscos analise os possíveis acontecimentos e suas consequências, antes de decidir o que será feito e quando será feito, a fi m de reduzir os riscos a um nível aceitável.

O processo de gestão de riscos de segurança da informação pode ser aplicado à organização como um todo, a uma área específica da organização (por exemplo, um departamento, um local físico, um serviço), a qualquer sistema de informações, a controles já existentes, planejados ou apenas a aspectos particulares de um controle (por exemplo, o plano de continuidade de negócios).

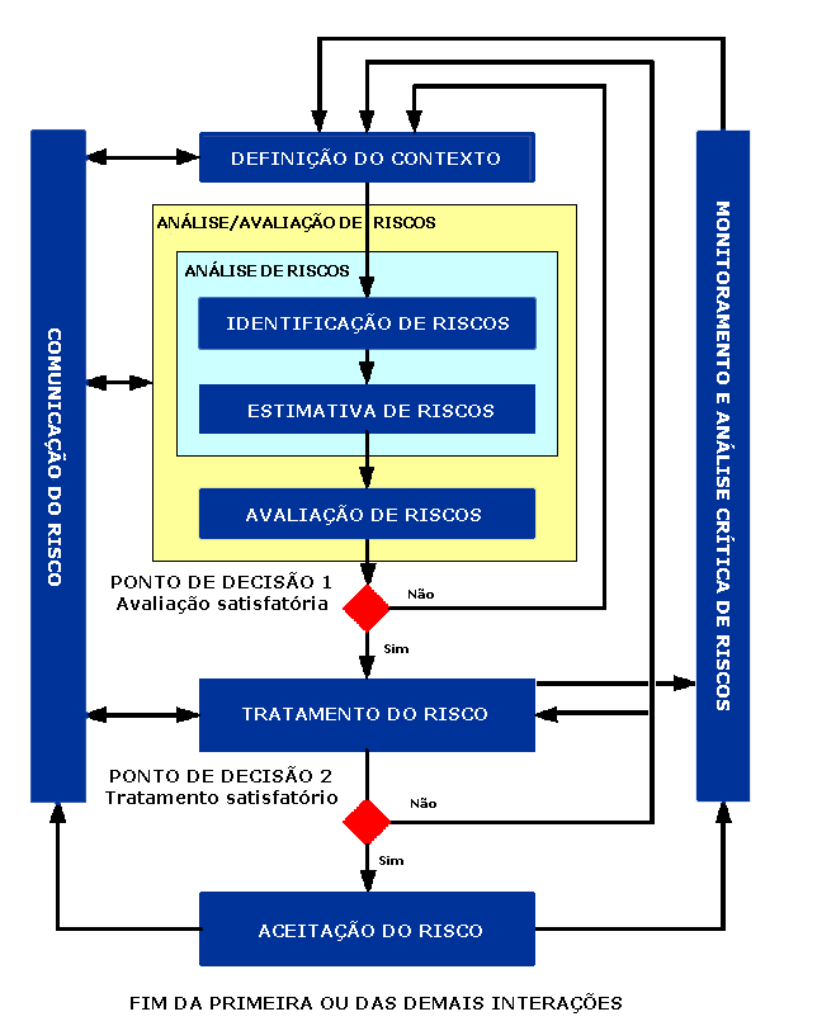
Gestão de Riscos em Segurança da Informação

Convém que a gestão de riscos de segurança da informação contribua para:

- A identificação de riscos
- O processo de avaliação de riscos em função das consequências ao negócio e da probabilidade de sua ocorrência
- A comunicação e entendimento da probabilidade e das consequências destes riscos
- O estabelecimento da ordem prioritária para tratamento do risco
- A priorização das ações para reduzir a ocorrência dos riscos
- A eficácia do monitoramento do tratamento dos riscos
- O monitoramento e análise crítica periódica dos riscos e do processo de gestão de riscos
- A coleta de informações de forma a melhorar a abordagem da gestão de riscos
- O treinamento de gestores e pessoal a respeito dos riscos e das ações para mitigá-los

Treinamento Básico em Segurança da Informação

Segundo a Norma ISO 27005 este é o Processo de Gestão de Riscos esquematizado:



Treinamento Básico em Segurança da Informação

DEFINIÇÃO DO CONTEXTO

Entrada: Todas as informações sobre a organização relevantes para a definição do contexto da gestão de riscos de segurança da informação.

Ação: Convém que o contexto externo e interno para gestão de riscos de segurança da informação seja estabelecido, o que envolve a definição dos critérios básicos necessários para a gestão de riscos de segurança da informação (7.2), a definição do escopo e dos limites (7.3) e o estabelecimento de uma organização apropriada para operar a gestão de riscos de segurança da informação (7.4).

AVALIAÇÃO DOS RISCOS

Entrada: Critérios básicos, o escopo e os limites, e a organização do processo de gestão de riscos de segurança da informação que se está definindo.

Ação: Convém que os riscos sejam identificados, quantificados ou descritos qualitativamente, priorizados em função dos critérios de avaliação de riscos e dos objetivos relevantes da organização.

AVALIAÇÃO DOS RISCOS

Diretrizes para implementação: Um risco é a combinação das consequências advindas da ocorrência de um evento indesejado e da probabilidade de sua ocorrência. O processo de avaliação de riscos quantifica ou descreve o risco qualitativamente e capacita os gestores a priorizar os riscos de acordo com a sua gravidade percebida ou com outros critérios estabelecidos.

O processo de avaliação de riscos consiste nas seguintes atividades:

- Identificação de riscos
- Análise de riscos
- Avaliação de riscos

Treinamento Básico em Segurança da Informação

AVALIAÇÃO DOS RISCOS EM SEGURANÇA DA INFORMAÇÃO

É a pedra fundamental da gestão de riscos. Procedimentos para estimar a probabilidade de ameaças e perdas que podem ocorrer devido a vulnerabilidade do sistema. O propósito é ajudar a detectar proteções de baixo custo e prover o nível de proteção necessário.
Fazem parte desta fase as seguintes etapas:

Identificação dos Riscos:
Introdução a Identificação dos Riscos
O propósito da Identificação de riscos é determinar eventos que possam causar uma perda potencial e deixar claro como, onde e por que a perda pode acontecer. As etapas descritas nas próximas subseções de 8.2 servem para coletar dados de entrada para a atividade de análise de riscos.

Convém que a Identificação de riscos inclua os riscos cujas fontes estejam ou não sob controle da organização, mesmo que a fonte ou a causa dos riscos não seja evidente.
.

TRATAMENTO DO RISCO EM SEGURANÇA DA INFORMAÇÃO

Existem quatro opções disponíveis para o tratamento do risco: reduzir, reter/aceitar, evitar ou transferir o risco.
Devem ser selecionadas proteções que diminuem certas ameaças.
Deve ser determinado um nível de risco tolerável e implementadas proteções de baixo custo para reduzir perdas em nível aceitável.
As proteções podem atuar de diversos modos:
– Reduzir a possibilidade de ocorrência de ameaças.
– Reduzir o impacto das ocorrências das ameaças.
– Facilitar a recuperação das ocorrências das ameaças.
Deve-se focalizar áreas que têm grande potencial para perdas.
As proteções devem ter boa relação custo-benefício, isto é, devem trazer mais retorno que os gastos com implementação e manutenção.

TRATAMENTO DO RISCO EM SEGURANÇA DA INFORMAÇÃO

Modificação do risco (redução)

Ação: Convém que o nível de risco seja gerenciado através da inclusão, exclusão ou alteração de controles, para que o risco residual possa ser reavaliado e então considerado aceitável.

Retenção do risco (aceitação)

Ação: Convém que as decisões sobre a retenção do risco, sem outras ações adicionais, sejam tomadas tendo como base a avaliação de riscos

Ação de evitar o risco (eliminação)

Ação: Convém que a atividade ou condição que dá origem a um determinado risco seja evitada.

Compartilhamento do risco (transferência)

Ação: Convém que um determinado risco seja compartilhado com outra entidade que possa gerenciá-lo de forma mais eficaz, dependendo da avaliação de riscos.

ACEITAÇÃO DO RISCO

A aceitação do risco deve ser formalmente registrada juntamente com a responsabilidade pela decisão de acordo com o ítem 6.1.3. da norma ISO 27001 que determina a obtenção da aprovação por parte da direção dos riscos residuais propostos.

Fim do Módulo 3

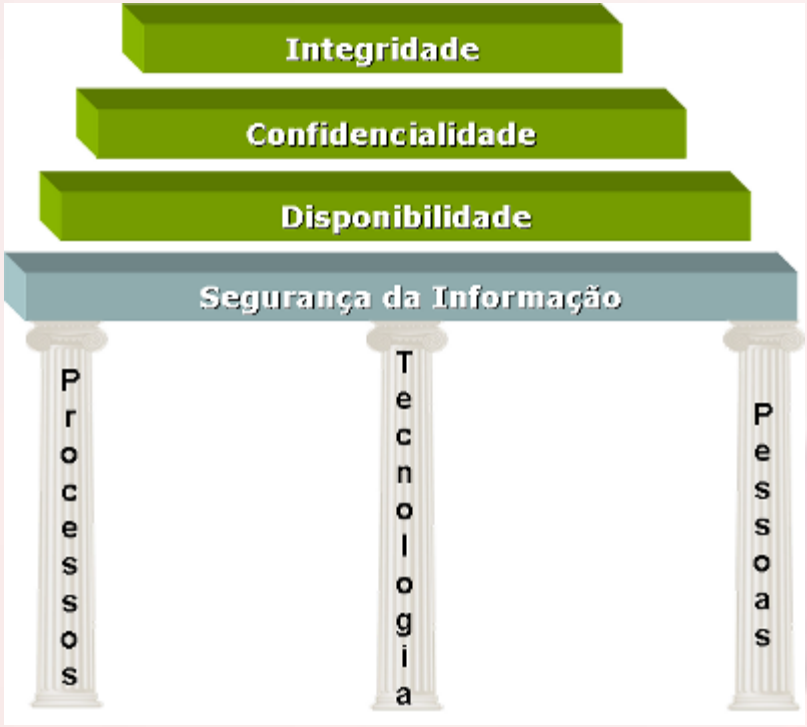
Gestão de Riscos em Segurança da Informação

Análise avaliação e tratamento de Riscos.

Aceitação de Riscos

Módulo 4

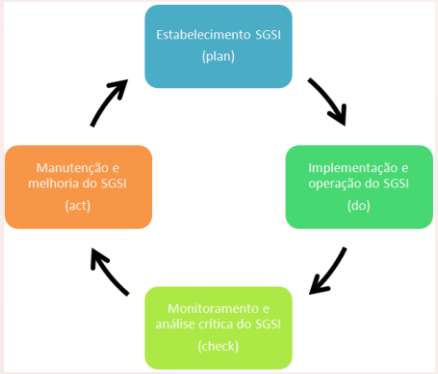
Sistema de Gestão da Segurança da Informação



Treinamento Básico em Segurança da Informação

Sistema de Gestão da Segurança da Informação

Um Sistema de Gestão de Segurança da Informação (SGSI) é um conjunto de políticas, processos e procedimentos, baseado em normas e na legislação, que uma organização implementa para prover segurança no uso de seus ativos de informação. Este sistema deve ser conhecido e seguido por todos aqueles que se relacionam direta ou indiretamente com a infra-estrutura de TI da organização, tais como: funcionários, prestadores de serviço, parceiros e terceirizados. O SGSI deve possuir obrigatoriamente o aval da direção e do departamento jurídico da organização para conferir sua legitimidade.



Treinamento Básico em Segurança da Informação

O Sistema de Gestão da Segurança da Informação é estruturado a partir do inventário de ativos de informação e gestão dos riscos em segurança da informação.

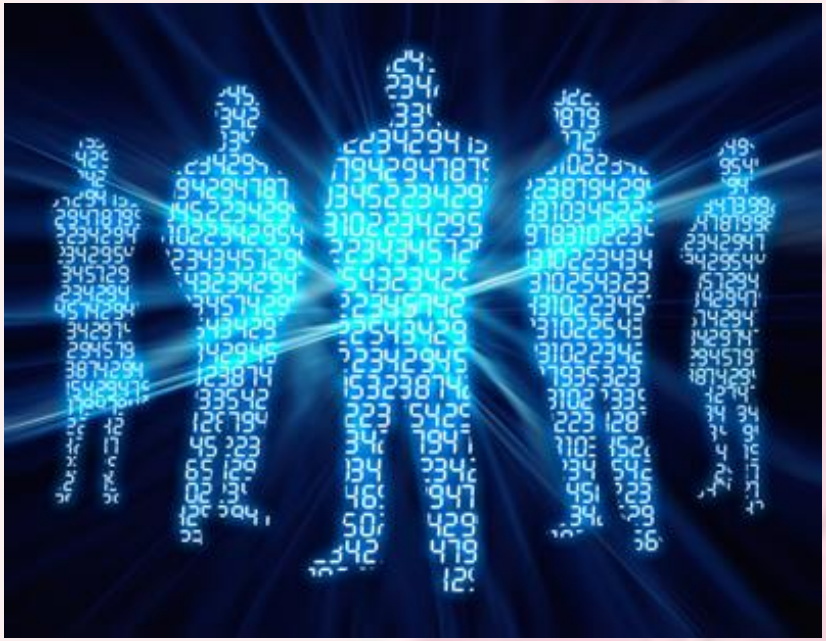
Ele pode ser definido como parte do sistema de gestão, baseado no enfoque de risco nos negócios, para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar a segurança da informação.

Este sistema deverá conter medidas técnicas, organizacionais e físicas que devem abranger as pessoas, os processos e a tecnologia pilares básicos de um sistema de gestão organizacional.

Treinamento Básico em Segurança da Informação

PESSOAS "QUEM SÃO ?"

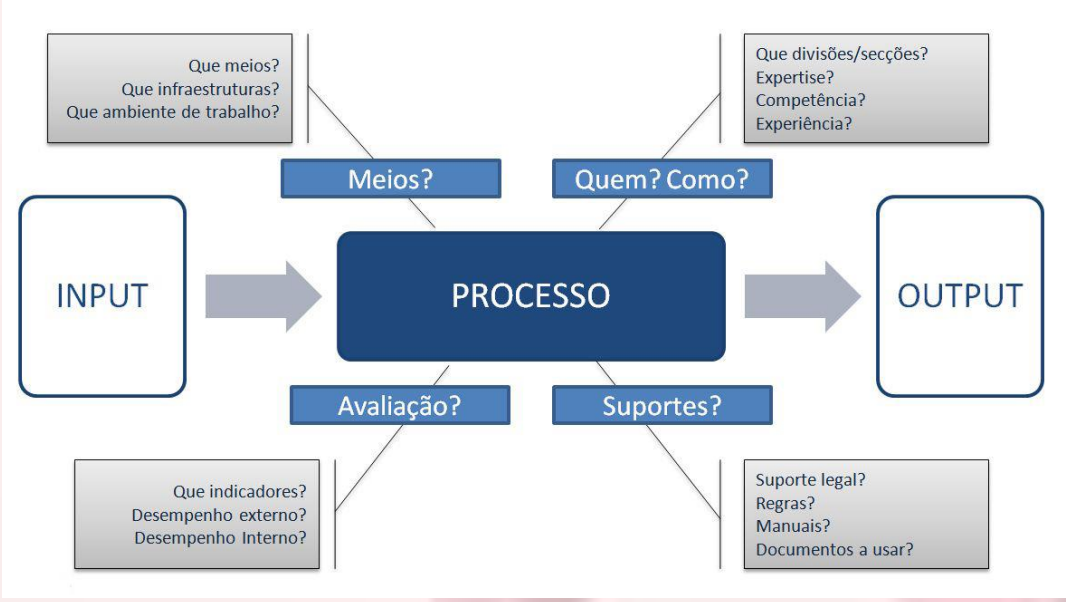
- Alta Administração
- Gestores;
- Servidores;
- Parceiros de Negócios;
- Provedores de Serviços;
- Terceirizados;
- Ciddãos;
- Fornecedores;
- Orgãos reguladores, etc.



PROCESSOS "O QUE NOS FAZEMOS ?"

Os processos referem-se às práticas de trabalho ou fluxo de trabalho. Os processos são compostos por passos repetíveis objetivando o atingimento dos objetivos de negócio. Processos típicos dentro de um Sistema de Gestão da Segurança da Informação são:

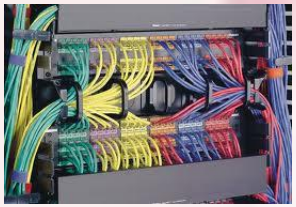
- Gestão de Riscos;
- Gestão de Incidentes em SI;
- Gestão de Problemas;
- Controle de Acesso Físico;
- Controle de Acesso Lógico;
- Gestão de Configuração;
- Gestão de Capacidade;
- Gestão de Níveis de Serviço;
- Help desk;



Treinamento Básico em Segurança da Informação

TECNOLOGIAS – “O QUE NOS USAMOS PARA MELHORAR O QUE FAZEMOS ?”

- Cabeamento estruturado;
- Redes de Voz e Dados;
- Servidores e estações de trabalho;
- Sistemas Operacionais;
- Aplicativos de Software;
- Equipamentos de comunicação;
- VPNs e ambientes virtuais;
- Serviços de acesso remoto;
- Redes Wireless;
- Smartphones, Tablets e Notebooks;
- etc...



Treinamento Básico em Segurança da Informação

SGSI:

Treinamento Básico em Segurança da Informação

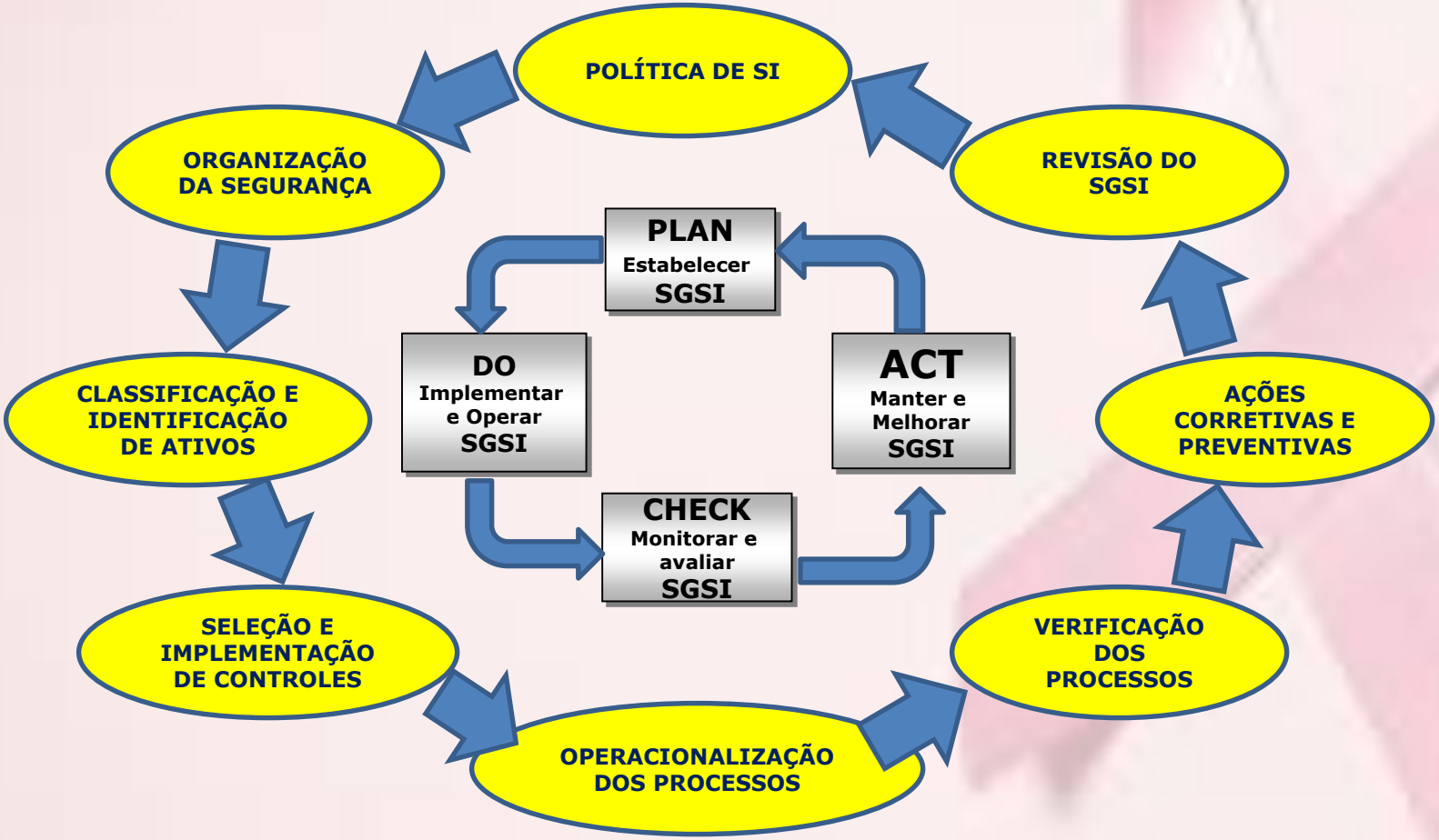
1. **Política de Segurança da Informação** para prover gerenciamento, direção e suporte para Segurança da Informação;
2. **Organização da Segurança da Informação** determina o modelo de gerenciamento da Segurança da Informação;
3. **Gestão de ativos** para garantir a segurança dos ativos de informação e outros relacionados, de acordo com o seu valor para a organização.
4. **Segurança em Recursos Humanos** para reduzir os riscos de erro humano, roubo, fraude ou utilização abusiva das instalações.
5. **Segurança física e ambiental** para impedir o acesso não autorizado, comprometimento, roubo ou danos aos ativos de informação e instalações de processamento da informação.

Treinamento Básico em Segurança da Informação

6. **Gerenciamento de Operações e Comunicações** para garantir o funcionamento correto e seguro das instalações de processamento da informação.
7. **Controle de Acesso** para controlar o acesso às informações e instalações de processamento da informação de forma que somente as pessoas autorizadas tenham este acesso.
8. **Aquisição, desenvolvimento e manutenção de Sistemas de Informação** para garantir que a segurança seja incorporada aos Sistemas de Informação.
9. **Gestão de Incidentes em Segurança da Informação** para garantir que os incidentes e fraquezas da segurança da informação sejam comunicados e tratados.
10. **Gestão da Continuidade dos negócios** para reduzir a possibilidade de descontinuidade operacional em casos de falhas de segurança ou desastre a níveis aceitáveis.
11. **Conformidade** para evitar a violação de leis, normas estatutárias, regulamentos, contratos ou normas de segurança~.

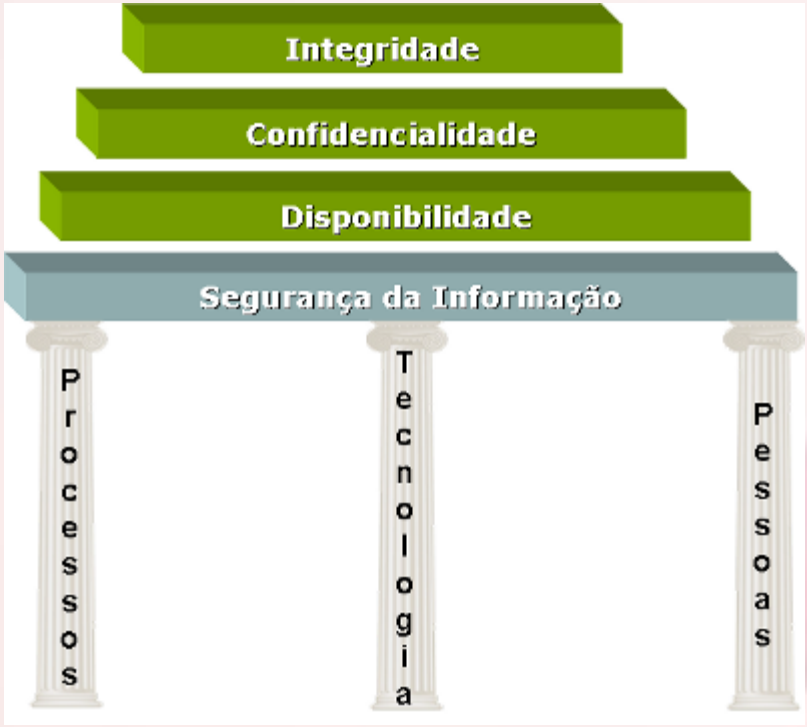
Treinamento Básico em Segurança da Informação

Implantando o SGSI:



FIM do Módulo 4

Sistema de Gestão da Segurança da Informação



Módulo 5

Segurança Física

Treinamento Básico em Segurança da Informação

Segurança física

Segurança física é parte da segurança da informação, pois todos os ativos do negócio também devem ser fisicamente protegidos. Segurança física é mais antiga do que a segurança da informação; apenas pense na proteção que um castelo proporciona aos que estão dentro dele. Proteger a informação se tornou importante muito mais tarde.

Treinamento Básico em Segurança da Informação

A Segurança física ...

Considera as ameaças físicas como incêndios, desabamentos, relâmpagos, alagamento, acesso indevido de pessoas, forma inadequada de tratamento e manuseio do material.

As medidas a serem adotadas em relação a Segurança Física, como já vimos, são resultantes do processo de gestão de riscos.

São exemplos de medidas em Segurança Física:

- Controle de acesso através de barreiras físicas;
- Monitoramento através de câmeras;
- Areas com entradas restritas;
- Sistemas de proteção contra incêndio e inundação;

Segurança física

- A segurança física deve considerar a proteção de equipamentos contra efeitos do clima e condições ambientais.
- A proteção das instalações em geral contra desastres naturais como incêndio, inundação, vazamentos de água, temporais, etc
- Cuidados com os cabeamentos lógicos e elétricos.

- Treinamento de pessoal de forma a assegurar que as medidas de segurança física surtam o efeito desejado.
- Definição clara das medidas nos acordos de confidencialidade e contratos com fornecedores e clientes.

Perímetros de Proteção

As medidas de segurança não devem restringirem-se às áreas de processamento da informação, devem ser adotadas de acordo com a sensibilidade dos ativos de informação e sua localização, portanto, devem começar fora da empresa.

O acesso aos ativos deve ter restrições de acordo com vários perímetros de segurança:

- Área externa a empresa
- Acesso aos prédios
- Áreas de trabalho;
- Áreas de processamento da informação e/ou ativos sensíveis ou com alto grau de confidencialidade.

Proteção contra incêndio

“ Incêndio se apaga no projeto ! “. Esta frase resume toda justificativa econômica e social que o tema reclama. A importância do planejamento nesta área é medida pelos sinistros evitados e não pelos incêndios extintos. Neste processo preventivo os projetistas têm participação fundamental. Apesar disto, a criação arquitetônica, e muitos dos projetos derivados, ainda são feitos à margem do conhecimento da ciência da prevenção contra o fogo.

A proteção contra incêndio tem regulamentações compulsórias e requisitos que devem ser atendidos no que se refere a:

Sinalização;

Equipe treinada;

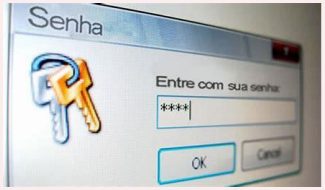
Agentes para extinção do incêndio;

Controle de Acesso Físico

Estudo dos métodos para reconhecimento unívoco de indivíduos através de suas características físicas e/ou comportamentais
“O que você é somente você é”
Características Fisiológicas e Comportamentais

Autenticação

Uma proteção que garanta a autenticidade deve ser realizadas em três camadas :
O que você sabe
O que você tem
O que você é



Treinamento Básico em Segurança da Informação

O que você sabe

O que você possui

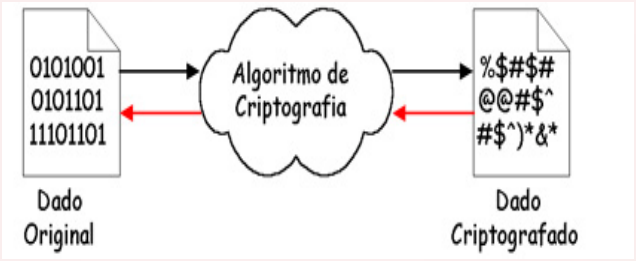
O que você é

Fim do Módulo 5

Segurança Física

Módulo 6

Medidas Técnicas



Segurança de Sistemas, medidas técnicas

Após o processo de gestão de riscos, além da determinação das medidas físicas a serem adotadas uma série de medidas técnicas são recomendadas para assegurar a proteção da informação, da infra-estrutura de TI e evitar o acesso indesejado por meio de controle de acesso e criptografia.

Controle de acesso lógico:

Os controles de acesso lógico são um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizado feitas por pessoas ou por outros programas de computador.

Treinamento Básico em Segurança da Informação

O que deve ser protegido ?

A proteção aos recursos computacionais inclui:

- Aplicativos – Programas fonte e objeto. O acesso não autorizado pode alteraras funções dos programas.
- Arquivos de dados – Bases de dados podem ser alteradas ou apagadas sem a autorização adequada.
- Utilitários e Sistema Operacional – O acesso também deve ser restrito, pois podem provocar alterações nas configurações e nos arquivos em geral ou podem permitir a cópia dos mesmos.
- Arquivos de Senhas – A falta de proteção a esses arquivos pode comprometer toda a segurança, já que se forem descobertos e decifrados, a vulnerabilidade é total.
- Arquivos de Log – Os logs são usados para registra as ações dos usuários, sendo ótimas informações para auditorias e análise de quebras de segurança. Se não houver proteção a esses arquivos, o usuário ou invasor pode apagar as pistas de suas ações.

Elementos **Básicos de Controle de Acesso Lógico**

Dois pontos distintos de controle: o recurso computacional que se pretende proteger e o usuário a quem se pretende conceder os privilégios e acesso aos recursos.

Objetivos dos controles:

- Apenas usuários autorizados podem ter acesso aos recursos.
- Os usuários devem ter acesso aos recursos necessários a execução de suas tarefas.
- O acesso a recursos críticos deve ser monitorado e restrito.
- Os usuários devem ser impedidos de executar transações incompatíveis com sua função ou responsabilidades.

Processo de Logon

- Obtenção de acesso aos aplicativos, dados e sistema computacional.
- Requer conta ou logon – identificação, e uma senha - autenticação.
- Usuários habilitados já devem conhecer o processo e o formato. Não é necessário "ajudas" toda vez que ele for "logar".
- É recomendável limitar o número de tentativas frustradas de logon, bloqueando a conta do usuário e desfazendo a conexão.
- Identificação do usuário – deve ser única. Regras de formação também são importantes que permitem rápida identificação.
- Autenticação do usuário – é a confirmação do usuário perante o sistema. Pode ser por senha, cartões ou características físicas, como o formato da mão, da retina ou do rosto, impressão digital ou reconhecimento da voz.

.

Treinamento Básico em Segurança da Informação

O que o usuário sabe:
login
senha

O que possui:
token

O que é:
Identificação biométrica

Treinamento Básico em Segurança da Informação

Senhas

Alguns softwares são capazes de quebrar senhas frágeis. Podem ser usados também para bloquear o uso delas.

Uma boa senha deve:

- Ser composta por letras (maiúsculas e minúsculas), números e símbolos;
- De fácil memorização;
- De digitação rápida;
- Evitar usar as mesmas senhas para vários sistemas, pois se um deles não for protegido, o risco é grande.
- Forçar ou criar um hábito de troca periódica.

Treinamento Básico em Segurança da Informação

Tokens

- Token é um objeto que o usuário possui que o diferencia das outras pessoas e o habilita a acessar alguma coisa.

- Chaves, cartões, objetos especiais são exemplos comuns de tokens.

- A desvantagem é que podem ser perdidos, roubados ou reproduzidos com facilidade.

- Os cartões inteligentes estão sendo muito usados e aperfeiçoados para uso cada vez mais abrangente.

Sistemas Biométricos

- São sistemas de verificação de identidade baseados em características físicas dos usuários.
- São mais difíceis de serem burlados;
- São a evolução dos sistemas manuais de reconhecimento, como análise grafológica e de impressões digitais.
- A tecnologia de medir e avaliar determinada característica de tal forma que o indivíduo seja realmente único.
- Um dos problemas é ainda a taxa de erros, pois determinada característica pode mudar em uma pessoa, com o passar dos anos ou por outra intervenção.

Treinamento Básico em Segurança da Informação

Sistemas Biométricos

- Impressões Digitais – São características únicas e consistentes. São armazenados de 40 a 60 pontos para verificar a identidade.
- Voz – Sistemas de reconhecimento de voz são usados para controle de acesso. Não são tão confiáveis em função dos erros causados por ruídos no ambiente ou problemas na voz do usuário.
- Geometria da Mão – usada em sistemas de controle acesso, porém essa característica pode ser alterada por aumento ou diminuição do peso ou artrite.
- Configuração da íris ou da retina – são mais confiáveis que as de impressão digital, através de direcionamento de feixes de luz nos olhos das pessoas.
- Reconhecimento Facial por meio de um termograma – Através de imagem tirada por câmera infravermelha que mostra os padrões térmicos de uma face. 19.000 pontos de identificação!

Proteção aos recursos

- O fato do usuário ter sido identificado e autenticado não quer dizer que ele poderá acessar qualquer informação ou aplicativo sem restrição.

- É necessário o controle específico, restringindo o acesso apenas às aplicações, arquivos e utilitários imprescindíveis às suas funções.

- Controles de menus, disponibilizando somente opções compatíveis com o usuário.

- Definição de perfis de cada usuário (ou grupo de usuários).

Monitoramento

•Registros de logs, trilhas de auditoria ou outros mecanismos de detecção de invasão são essenciais.

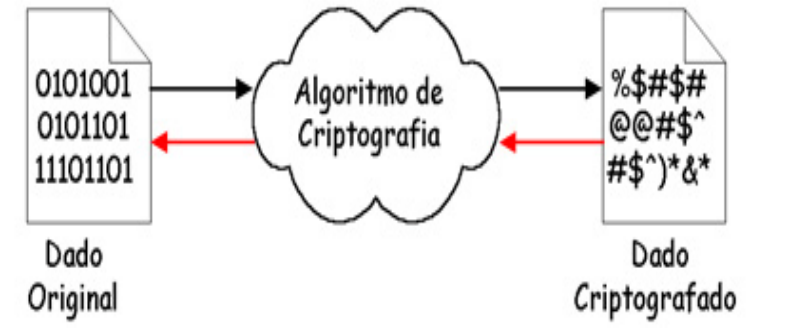
• Na ocorrência de uma invasão, erro ou atividade não autorizada, é imprescindível reunir evidências para se tomar medidas corretivas necessárias.

• Os logs funcionam também como trilhas de auditorias, registrando cronologicamente as atividades do sistema.

- Possibilitam a reconstrução, revisão ou análise dos ambientes e atividades relativas a uma operação, procedimento ou evento.
- Por conterem informações essenciais para a segurança, os arquivos de logs devem ser protegidos contra destruição ou alteração por usuários ou invasores.
- O uso em excesso também pode degradar o sistema, sendo necessário balancear a necessidade de registro de atividades criticas e os custos em termos de desempenhos.

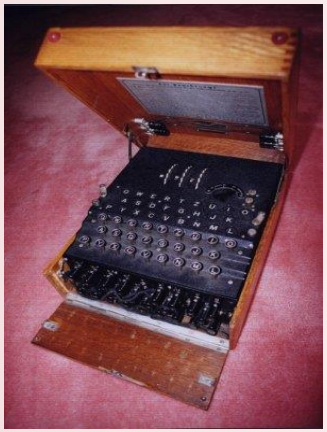
Criptografia

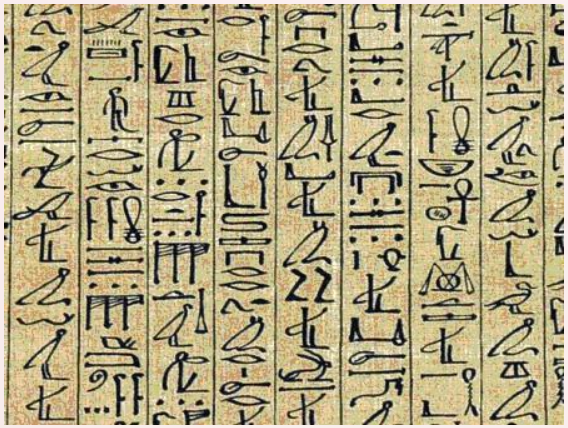
O uso de técnicas criptográficas tem como propósito prevenir algumas falhas de segurança num sistema de computadores.
Kriptos (em grego) = Secreto + Grafia (de escrever)
Criptografia = Escrita secreta.
Os procedimentos de criptografar e decriptografar são obtidos através de um algoritmo e uma chave.



Criptografia na História

- Egípcios antigos cifravam alguns de seus hieróglifos
- O barro de *Phaistos* (1600 a.c) ainda não decifrado
- Cifrador de Júlio César, aproximadamente 60 ac
- Tratado sobre criptografia por Trithemius entre 1500 e 1600

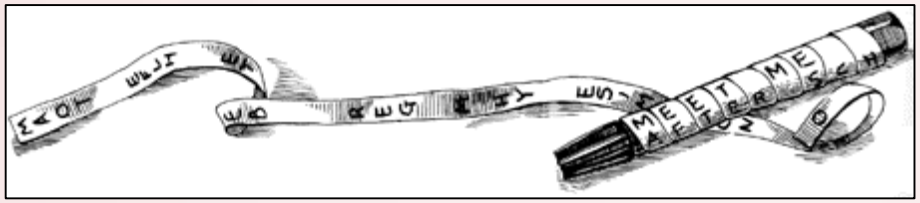




Treinamento Básico em Segurança da Informação

487 a.C. - Bastão de Licurgo

O remetente escreve a mensagem ao longo do bastão e depois desenrola a tira, a qual então se converte numa sequência de letras sem sentido. O mensageiro usa a tira como cinto, com as letras voltadas para dentro. O destinatário, ao receber o "cinto", enrola-o no seu bastão, cujo diâmetro é igual ao do bastão do remetente. Desta forma, pode ler a mensagem.



50 a.C. - Código de César

Cada letra da mensagem original é substituída pela letra que a seguia em três posições no alfabeto: a letra A substituída por D, a B por E, e assim até a última letra, cifrada com a primeira. Único da antiguidade usado até hoje, apesar de representar um retrocesso em relação à criptografia existente na época.**Denominação atual para qualquer cifra baseada na substituição cíclica do alfabeto: Código de César**.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

Criptografia em rede (computadores)

A mensagem é criptografada usando-se algoritmos.
Com o advento da internet e sua popularização, a criptografia em rede tem sido responsável pelo surgimento/fortalecimento do comércio eletrônico.

Exemplos:

- O DES (*Data Encryption Standard*), da IBM
- O RSA (**R**onald Rivest, Adi **S**hamir e Leonard **A**dleman)
- O PGP (*Pretty Good Privacy*), de Phil Zimmerman
- outras codificações (nas telecomunicações: celulares, satélites, etc.)

Certificação Digital

Sub-área da disciplina de **Criptografia**

Várias aplicações práticas

- Historicamente, **sigilo militar e diplomático**
- **Sigilo de comunicações** em geral
- **Detecção de adulterações**
  - Reforça a “força de prova” de um documento eletrônico
- **Identificação de usuários**
  - Substitui nome+senha

Assinatura Digital

Objetivo maior: conferir ao documento eletrônico **eficácia probante** equivalente ou superior a um documento em papel.

- Resistência a adulteração cientificamente periciável;
- Identifica o signatário;

Viabiliza realizar **seguramente por meios totalmente eletrônicos** uma série de trâmites formais que antes só eram concebíveis em papel.

- Celeridade nos processos, conveniência e ação à distância (onde apropriado).

Certificado Digital

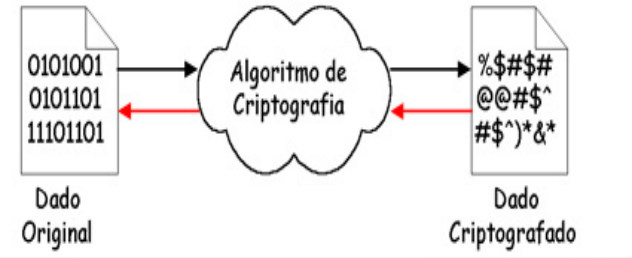
Objetivo maior: **identificar os signatários**, estabelecendo a correspondência entre as chaves públicas (suas "identidades virtuais") e suas identidades institucionais/civis/etc no "mundo real".

Não apenas diz o nome do titular,...

...mas também demonstra (pericialmente, se necessário)

Fim do Módulo 6

Medidas Técnicas



Módulo 7

Medidas Organizacionais

Política de Segurança da Informação, Recursos Humanos, Continuidade dos Negócios e Processos Operacionais

Política de Segurança da Informação

- De acordo com o RFC 2196 (*The Site Security Handbook*), uma política de segurança consiste num conjunto formal de regras que devem ser seguidas pelos utilizadores dos recursos de uma organização.
- As políticas de segurança devem ter implementação realista, e definir claramente as áreas de responsabilidade dos utilizadores, do pessoal de gestão de sistemas e redes e da direção. Deve também adaptar-se a alterações na organização. As políticas de segurança fornecem um enquadramento para a implementação de mecanismos de segurança, definem procedimentos de segurança adequados, processos de auditoria à segurança e estabelecem uma base para procedimentos legais na sequência de ataques.
- O documento que define a política de segurança deve deixar de fora todos os aspectos técnicos de implementação dos mecanismos de segurança, pois essa implementação pode variar ao longo do tempo. Deve ser também um documento de fácil leitura e compreensão, além de resumido.

Hierarquia de Documentos

O Sistema de Gestão da Segurança da Informação tem uma estrutura hierárquica de documentos, dentro dos seguintes níveis:

1. Política de Segurança da Informação
2. Políticas Específicas como: Utilização de Internet, e-mail, backup, etc
3. Procedimentos
4. Instruções de Serviço
5. Registros

Treinamento Básico em Segurança da Informação

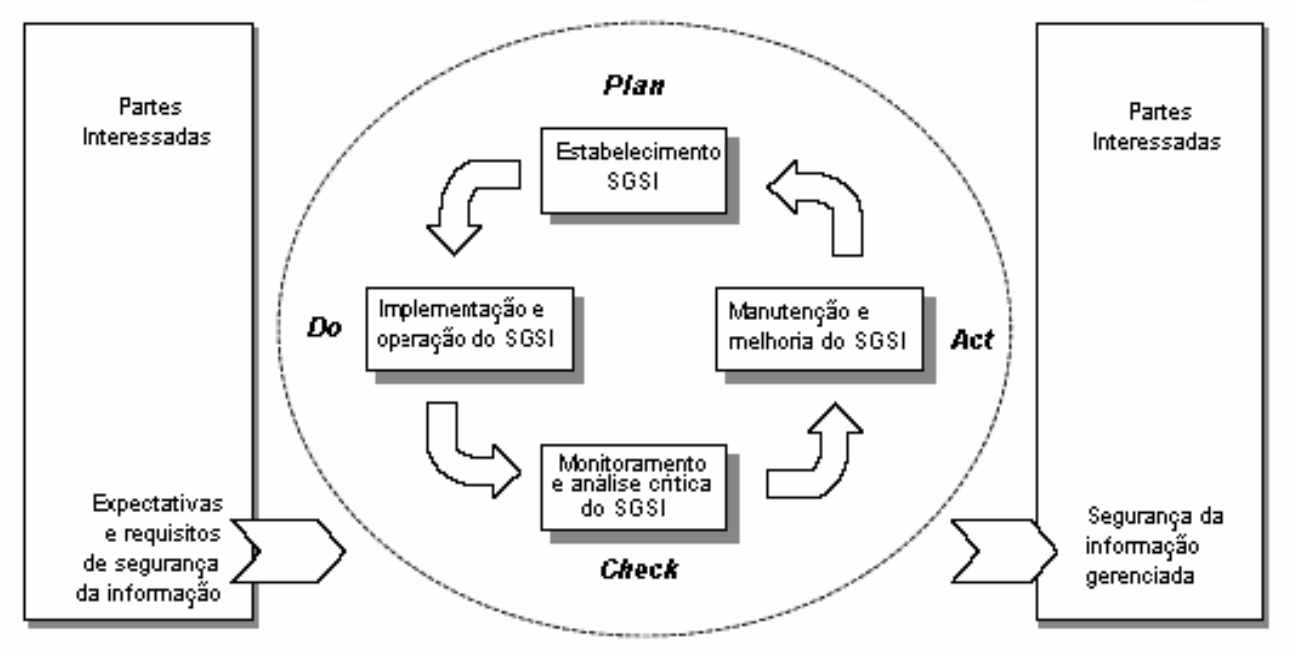
O SGSI, estrutura a Segurança da Informação em 11 domínios.
Um domínio é um conjunto de temas conectados logicamente e pertencentes a uma determinada área organizacional.

A norma ISO 27001 está estruturada dentro dos seguintes domínios:

A.5. POLÍTICA DE SEGURANÇA
A.6. ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO
A.7. GESTÃO DE ATIVOS
A.8. SEGURANÇA EM RECURSOS HUMANOS
A.9. SEGURANÇA FÍSICA E DO AMBIENTE
A.10. GERENCIAMENTO DAS OPERAÇÕES E COMUNICAÇÕES
A.11. CONTROLE DE ACESSO
A.12. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS
A.13. GESTÃO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO
A.14. GESTÃO DA CONTINUIDADE DO NEGÓCIO
A.15. CONFORMIDADE

Treinamento Básico em Segurança da Informação

POLÍTICA DE SEGURANÇA - A Política de Segurança da Informação e o SGSI estão em constante processo de avaliação e melhoria contínua.

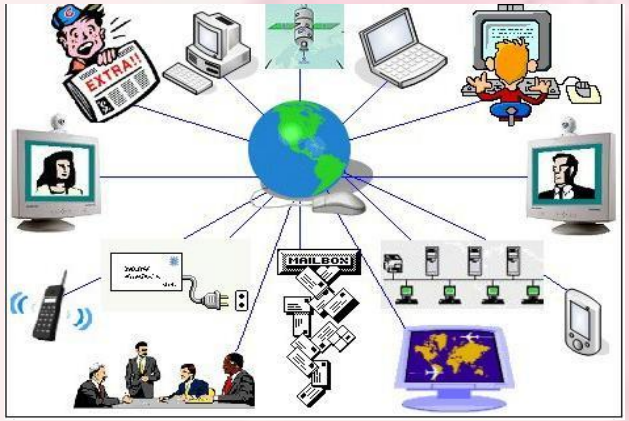


Treinamento Básico em Segurança da Informação

ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO - Apesar da Segurança da Informação, ser uma responsabilidade de todos na organização, é fundamental que este processo seja controlado e que uma estrutura responsável pelo controle esteja definida de forma bem clara e com respaldo da alta direção.

Treinamento Básico em Segurança da Informação

GESTÃO DE ATIVOS - Ativos representam todos os itens da organização onde informações são criadas, processadas, armazenadas, transmitidas ou descartadas. O gerenciamento de ativos é fundamental para priorizar investimentos e concentrar esforços nos ativos mais críticos, que sustentam os processos da organização. É a partir do gerenciamento de riscos dos ativos de informação que todos os procedimentos de segurança são definidos. Dentro das medidas organizacionais, o processo de gestão de ativos que engloba o inventário dos ativos de informação, sua classificação e determinação de importância. Já o processo de gestão de riscos faz a análise e tratamento dos riscos em Segurança da Informação.



Treinamento Básico em Segurança da Informação

SEGURANÇA EM RECURSOS HUMANOS -Em relação aos Recursos Humanos dentro da organização é fundamental que processos como: admissão, transferência de setor/departamento e demissão, tenham preocupação com procedimentos relativos a Segurança da Informação , por exemplo:

- Considerando a formalização de acordos de confidencialidade quando da contratação;
- Considerando a mudança de configuração de acesso quando da transferência de setor/departamento;
- Considerando a revogação de privilégios de acesso quando da demissão, etc.

Treinamento Básico em Segurança da Informação

SEGURANÇA FÍSICA E DO AMBIENTE E CONTROLE DE ACESSO– Em grandes organizações as medidas de controle de acesso são fundamentais para assegurar a segurança física. Medidas como controle e registro de entradas e obrigatoriedade de acompanhamento de visitantes por funcionários asseguram este tipo de segurança. Todas as medidas para garantir a segurança devem estaqr estruturadas em procedimentos organizacionais bem divulgados e conhecidos por todos na organização.

Treinamento Básico em Segurança da Informação

GESTÃO DA CONTINUIDADE DO NEGÓCIO : A continuidade operacional assegurada, é um dos grandes objetivos de um SGSI, e para assegurá-la, os planos de contingência e de recuperação de desastres são de extrema importância .

Tanto os planos de continuidade de negócios como os de recuperação de desastres devem considerar diversos fatores, eles devem ser aprovados pela diretoria e testados periodicamente, isso quer dizer que todos os funcionários devem saber o que fazer nos casos de contingência. Sempre que mudanças ocorrerem na organização o seu impacto em relação aos planos devem ser analisados. É importante considerar que tanto pessoas como equipamentos podem ser afetados por um desastre, portanto um plano de continuidade de negócios deve prever uma eventual substituição.

Treinamento Básico em Segurança da Informação

GESTÃO DE OPERAÇÕES E COMUNICAÇÕES: Com o objetivo de manter uma gestão eficaz nas operações e comunicações de TI, a segurança da informação requer a documentação dos procedimentos para operação dos diversos equipamentos bem como a inclusão de todos os detalhes necessários em instruções de serviços e manuais de operação.

Um procedimento operacional documentado, deve considerar: como lidar com a informação, periodicidade de realização de cópias de segurança, procedimentos a serem adotados em caso de incidentes, formas de rastreamento e auditoria

Treinamento Básico em Segurança da Informação

Os seguintes processos são de fundamental importância ao atingimento da Segurança da Informação :

- Gerenciamento de Mudanças;
- Gerenciamento de Serviços de Terceiros;
- Gerenciamento de Nível de Serviço;
- Gerenciamento de Incidentes em SI;
- Gerenciamento de Problemas em SI;

Fim do Módulo 7

Medidas Organizacionais

Política de Segurança da Informação, Recursos Humanos, Continuidade dos Negócios e Processos Operacionais

Treinamento Básico em Segurança da Informação

Módulo 8

Legislação e Regulamentações

Leis , Regulamentos, Normas Técnicas, Direitos Autorais, Auditorias, Observação de Políticas, Prevenção de abuso das instalações.

Treinamento Básico em Segurança da Informação

A principal meta de qualquer organização é o atingimento dos objetivos do negócio. Com a implementação da Governança Coorporativa e subsequentemente da Governança em TI, busca-se o alinhamento dos objetivos da área de Tecnologia da Informação com os objetivos estratégicos. No entanto é necessário a observância de leis, regulamentos e obrigações contratuais.

A área de Segurança da Informação deve considerar todos os aspectos que envolvem as obrigações legais e contratuais relativas a segurança, como:

- Constituição Federal quando trata do direito à privacidade e sigilo;
- Leis Federais que dispõe sobre propriedade intelectual de software, obrigatoriedade de Política de Segurança da Informação;
- Proibição de acesso a sites que tratam de assuntos considerados crimes como: racismo, nazismo, pedofilia, etc..;
- Obrigações contratuais assumidas com terceiros;
- Legislação sobre Segurança da Informação do Governo Federal, Leis, Portarias do GSI/DSIC, Instruções Normativas do GSI/DSIC, Normas Complementares GSI/DSIC

Treinamento Básico em Segurança da Informação

A conformidade esta relacionada com algo que uma organização deve atender, é o caso das leis, normas e regulamentos. Algumas vezes podem haver conflitos , como nos casos das multinacionais que devem cumprir leis locais e internacionais por exemplo, as leis relativas a privacidade são diferentes entre países da Europa e Estados Unidos.

A conformidade envolve também a observância de padrões internacionais como as normas ISO relativas a Segurança da Informação e Qualidade.

A implementação de um SGSI, com políticas e procedimentos que favoreçam o cumprimento das normas, regulamentos e leis é um indicativo de CONFORMIDADE.

Sistema de Gestão da Segurança da Informação e Comunicações: o que deve ser desenvolvido para o atingimento da conformidade nesta área pelos órgãos da administraçã publica federal ?

1. Definir uma política para sistema de gestão da segurança da informação

O Sistema de Gestão da Segurança da Informação, abrange basicamente três níveis de documento, as Políticas no topo da pirâmide, as normas no segundo nível e os procedimentos e registros no terceiro nível deve-se estabelecer uma política do Sistema de Gestão da Segurança da Informação que contenha objetivos, processos e procedimentos relevantes para o gerenciamento de riscos e a melhoria da segurança da informação de forma a entregar resultados de acordo com o planejamento estratégico da instituição.

Enquanto a POSIC define com é tratada a Segurança da Informação da Organização a Política do SGSI estabelece como todo o Sistema de Gestão deve ser estruturado e mantido. A periodicidade de atualização e eventuais gatilhos.

2. Definir o escopo da segurança da informação

É importante a definição do escopo da segurança da informação até como forma de planejar a implementação do sistema, priorizando-se os processos mais críticos. É importante atentar que a segurança da informação abrange todos os ativos de informação de uma organização como: recursos tecnológicos, processos, pessoas, informações armazenadas em todos os meios, equipamentos, etc.

Tendo em vista a amplitude e dinamicidade dos ativos de informação, os organismos certificadores estabelecem a certificação dentro do escopo definido pela organização, portanto é de fundamental importância a delimitação de todas as fronteiras.

3. Definir e nomear os responsáveis pela segurança da informação na instituição

Segundo a IN 01 GSI/DSIC em seu Art. 5º, aos demais órgãos e entidades da Administração Pública Federal, direta e indireta, em seu âmbito de atuação, compete:

I - coordenar as ações de segurança da informação e comunicações;

II - aplicar as ações corretivas e disciplinares cabíveis nos casos de quebra de segurança; III - propor programa orçamentário específico para as ações de segurança da informação e comunicações;

IV - nomear Gestor de Segurança da Informação e Comunicações;

V - instituir e implementar equipe de tratamento e resposta a incidentes em redes computacionais;

VI - instituir Comitê de Segurança da Informação e Comunicações;

a) Atribuições do Comitê de Segurança da Informaçao e Comunicações

"Art. 6º Ao Comitê de Segurança da Informação e Comunicações, de que trata o inciso VI do art. 5º, em seu âmbito de atuação, compete:

I - assessorar na implementação das ações de segurança da informação e comunicações;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

III - propor alterações na Política de Segurança da Informação e Comunicações; e

IV - propor normas relativas à segurança da informação e comunicações.

b) Atribuições do Gestor de Segurança da Informaçao e Comunicações

Art. 7º Ao Gestor de Segurança da Informação e Comunicações, de que trata o inciso IV do art. 5º, no âmbito de suas atribuições, incumbe:

I - promover cultura de segurança da informação e comunicações;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - propor recursos necessários às ações de segurança da informação e comunicações;

IV - coordenar o Comitê de Segurança da Informação e Comunicações e a equipe de tratamento e resposta a incidentes em redes computacionais;

b) Atribuições do Gestor de Segurança da Informaçao e Comunicações

Art. 7º Ao Gestor de Segurança da Informação e Comunicações, de que trata o inciso IV do art. 5º, no âmbito de suas atribuições, incumbe:

(....)

V - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;

VI - manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;

VII - propor normas relativas à segurança da informação e comunicações;

c) Definir a POSIC - Política de Segurança da Informação e Comunicações

Considerando o que estabelece a Norma Complementar nº 03/IN01/DSIC/GSIPR, Diretrizes para a Elaboração de Política de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal esta norma estabelece:

"5.1 Recomenda-se que para a elaboração da POSIC seja instituído um Grupo de Trabalho constituído por representantes dos diferentes setores do órgão ou entidade da APF, como por exemplo: segurança patrimonial, tecnologia da informação, recursos humanos, jurídico, financeiro e planejamento;

5.2 A elaboração da POSIC deve levar em consideração a natureza e finalidade do órgão ou entidade da APF, alinhando-se sempre que possível à sua missão e ao planejamento estratégico;

5.3 Recomenda-se que na elaboração da POSIC sejam incluídos os seguintes itens:

5.3.1 Escopo: neste item recomenda-se descrever o objetivo e abrangência da Política de Segurança da Informação e Comunicações, definindo o limite no qual as ações de segurança da informação e comunicações serão desenvolvidas no órgão ou entidade da APF;

5.3.2 Conceitos e definições: neste item recomenda-se relacionar todos os conceitos e suas definições a serem utilizados na Política de Segurança da Informação e Comunicações do órgão ou entidade da APF que possam gerar dificuldades de interpretações ou significados ambíguos;

5.3.3 Referências legais e normativas: neste item recomenda-se relacionar as referências legais e normativas utilizadas para a elaboração da Política de Segurança da Informação e Comunicações do órgão ou entidade da APF;

Treinamento Básico em Segurança da Informação

5.3.4 Princípios: neste item recomenda-se relacionar os princípios que regem a segurança da informação e comunicações no órgão ou entidade da APF;

5.3.5 Diretrizes Gerais: neste item recomenda-se estabelecer diretrizes sobre, no mínimo, os seguintes temas, considerando as Normas específicas vigentes no ordenamento jurídico:

a) Tratamento da Informação;

b) Tratamento de Incidentes de Rede;

c) Gestão de Risco;

d) Gestão de Continuidade;

e) Auditoria e Conformidade;

f) Controles de Acesso;

g) Uso de e-mail; e

h) Acesso a Internet.

5.3.7 Competências e Responsabilidades: neste item recomendam-se os seguintes procedimentos:

5.3.7.1 Definir a estrutura para a Gestão da Segurança da Informação e Comunicações;

5.3.7.2 Instituir o Gestor de Segurança da Informação e Comunicações do órgão ou entidade da APF, dentre servidores públicos civis ou militares, conforme o caso,

5.3.7.3 Instituir o Comitê de Segurança da Informação e Comunica

5.3.7.4 Instituir a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais do órgão ou entidade da APF.

5.3.8 Atualização: neste item recomenda-se estabelecer a periodicidade da revisão da Política de Segurança da Informação e Comunicações ou dos instrumentos normativos gerados a partir da própria POSIC.

5.4 A POSIC precisa ser objetiva, simples, de fácil leitura e entendimento;

5.5 A POSIC poderá ser complementada por Normas e Procedimentos que a referenciem.”

d) Definir a Metodologia de Gestão de Riscos

A metodologia de Gestão de Riscos deve seguir as orientações contidas na Norma Complementar nº 04/IN01/DSIC/GSIPR, e seu anexo, (Revisão 01) Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicações - GRSIC nos órgãos e entidades da Administração Pública Federal e na Norma ISO IEC 27005;

d) Realizar Inventário dos Ativos de Informação

O inventário de ativos a ser realizado deve seguir as orientações expressas na Norma Complementar nº10/IN01/DSIC/GSIPR, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

e) Definir a Declaração de Aplicabilidade

DEFINIR A DECLARAÇÃO DE APLICABILIDADE: formalizar a Declaração de Aplicabilidade segundo a Norma Complementar nº 02/IN01/DSIC/GSIPR, Metodologia de Gestão de Segurança da Informação e Comunicações.(Publicada no DOU Nº 199, de 14 Out 2008 - Seção 1) que estabelece:

- Os objetivos e os recursos necessários para cada ação de segurança da informação e comunicações selecionada e as razões para sua seleção;
- Os objetivos de cada ação de segurança da informação e comunicações que já foram implementadas em seu órgão ou entidade;
- Um resumo das decisões relativas à gestão de riscos;
- Justificativas de possíveis exclusões de ações de segurança da informação e comunicações sugeridas pelo Gestor de Segurança da Informação e Comunicações e não autorizadas pela autoridade decisória de seu órgão ou entidade.

e) Definir as Normas

- Continuidade dos Negócios segundo a **Norma Complementar nº 06/IN01/DSIC/GSIPR**, Estabelece Diretrizes para Gestão de Continuidade de Negócios, nos aspectos relacionados à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF;
- Tratamento da Informação segundo a **Norma Complementar nº 20/IN01/DSIC/GSIPR**, **(Revisão 01)**Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta
- Utilização de Dispositivos Móveis segundo a **Norma Complementar nº 12/IN01/DSIC/GSIPR**, Estabelece diretrizes e orientações básicas para o uso de dispositivos móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

e) Definir as Normas (continuação)

- Controles de Acesso segundo a **Norma Complementar nº 07/IN01/DSIC/GSIPR**, (Revisão 01) Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta
- Desenvolvimento de Sistemas estruturantes segundo a **Norma Complementar nº 19/IN01/DSIC/GSIPR**, Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta;
- Desenvolvimento de Software seguro segundo a **Norma Complementar nº 16/IN01/DSIC/GSIPR**, Estabelece as Diretrizes para o Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta;

e) Definir as Normas (continuação)

- Utilização de Computação em Nuvem segundo a **Norma Complementar nº 14/IN01/DSIC/GSIPR**, Estabelece diretrizes para a utilização de tecnologias de Computação em Nuvem, nos aspectos relacionados à Segurança da Informação e Comunicações (SIC), nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

e) Definir Procedimentos

- Utilização de Redes Sociais segundo a **Norma Complementar nº 15/IN01/DSIC/GSIPR**, Estabelece diretrizes de Segurança da Informação e Comunicações para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta;
- Testes dos Planos de Continuidade garantindo a efetividade dos Planos de Continuidade dos negócios, estes testes podem ser setorizados ou realizados por processos críticos;
- Gestão de Incidentes segundo a **Norma Complementar nº 08/IN01/DSIC/GSIPR**, Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal;

e) Definir Procedimentos (continuação)

- Gestão de Mudanças segundo a **Norma Complementar nº 13/IN01/DSIC/GSIPR**, Estabelece diretrizes para a Gestão de Mudanças nos aspectos relativos à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal, direta e indireta (APF)
- Controle de Registros segundo a **Norma Complementar nº 21/IN01/DSIC/GSIPR**, Estabelece as Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes nos órgãos e entidades da Administração Pública Federal, direta e indireta.
- Auditoria de Segurança da Informação de acordo com a **Norma Complementar nº 10/IN01/DSIC/GSIPR**, Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

e) Definir Procedimentos (continuação)

- Termo de Confidencialidade e Responsabilidade a todos servidores, prestadores de serviço e usuários de acordo com o escopo de seu acesso;
- Normas de Segurança da Contratação ao Desligamento de Servidores
- Gestão de Terceirizados assegurando o comprometimento e conhecimento das políticas e normas relativas a Segurança da Informação e Comunicações pertinentes ao serviço desempenhado;
- Utilização da Internet definindo os limites tolerados e como é realizado o monitoramento;
- Utilização de Correio Eletrônico institucional definir limites, procedimentos de backup/operação e responsabilidades do usuário;

E com todas estas implementações estaremos 100 % seguros ?

Treinamento Básico em Segurança da Informação

Treinamento Básico em Segurança da Informação

Confidencialidade	• Assegurar que a informação é acessível somente por aqueles devidamente autorizados
Integridade	• Salvaguardar a veracidade e complementariedade da informação bem como os seus métodos de processamento
Disponibilidade	• Assegurar que quem devidamente autorizado tem acesso á informação e bens associados sempre que necessário

Treinamento Básico em Segurança da Informação

manoel.fonseca@saude.gov.br