EXIN Information Security Foundation

com base na ISO/IEC 27001

Muito obrigado por escolher um treinamento oficial do Portal do Treinamento !

PORTAL DO TREINAMENTO!

EDUCAÇÃO EM TI

Cursos

DPO - Data Protection Officer

Governança de TI

ITIL 4

Lean IT

Agile

VeriSM

https://www.portaldotreinamento.com.br/

follow us on facebook

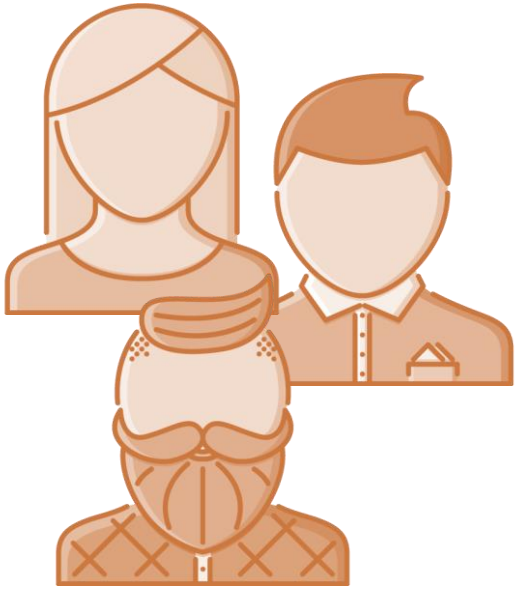
Follow us on Instagram

Follow us on LinkedIn

PORTAL DO TREINAMENTO!

LEMBRETES IMPORTANTES

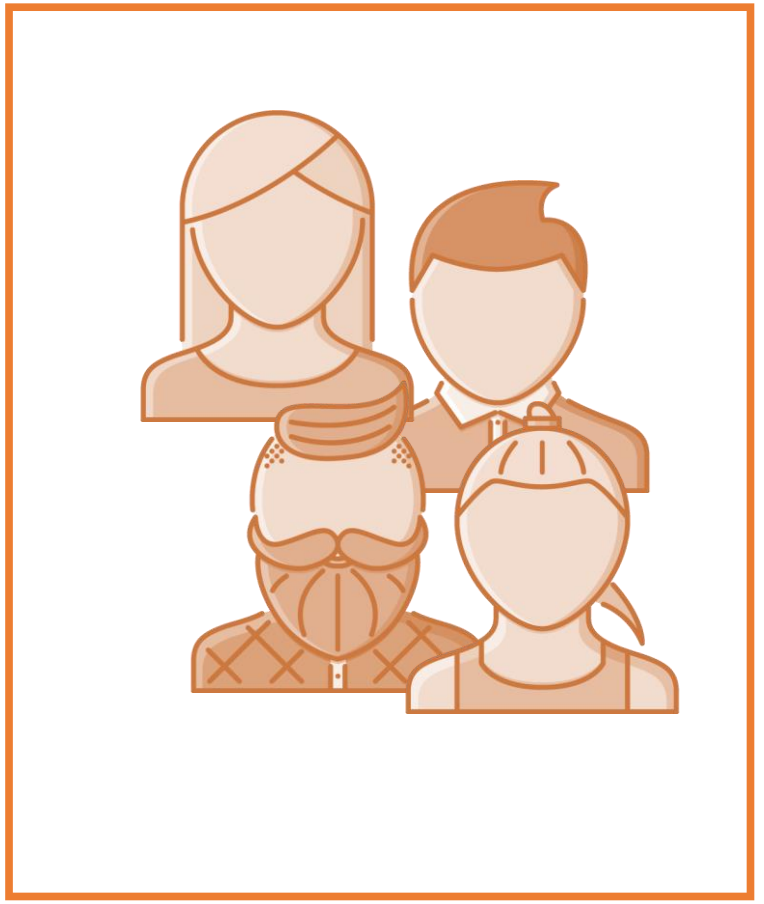
- Celulares em modo silencioso
- Dúvidas a qualquer momento
- Participação é recomendável
- Use seu conhecimento e o cenário de sua empresa
- Reler o material visto e ler o material para a próxima aula
- Divirta-se



PORTAL DO TREINAMENTO!

APRESENTAÇÃO

- Nome
- Bairro/Cidade
- Empresa
- Papel
- Certificações
- Quando pretende fazer o exame de certificação
- Hobby ou habilidade



OBJETIVOS DO CURSO

Dar aos participantes uma compreensão sobre segurança da informação, tendo como a base a norma ISO/IEC 27001 .

Este curso se destinada a :

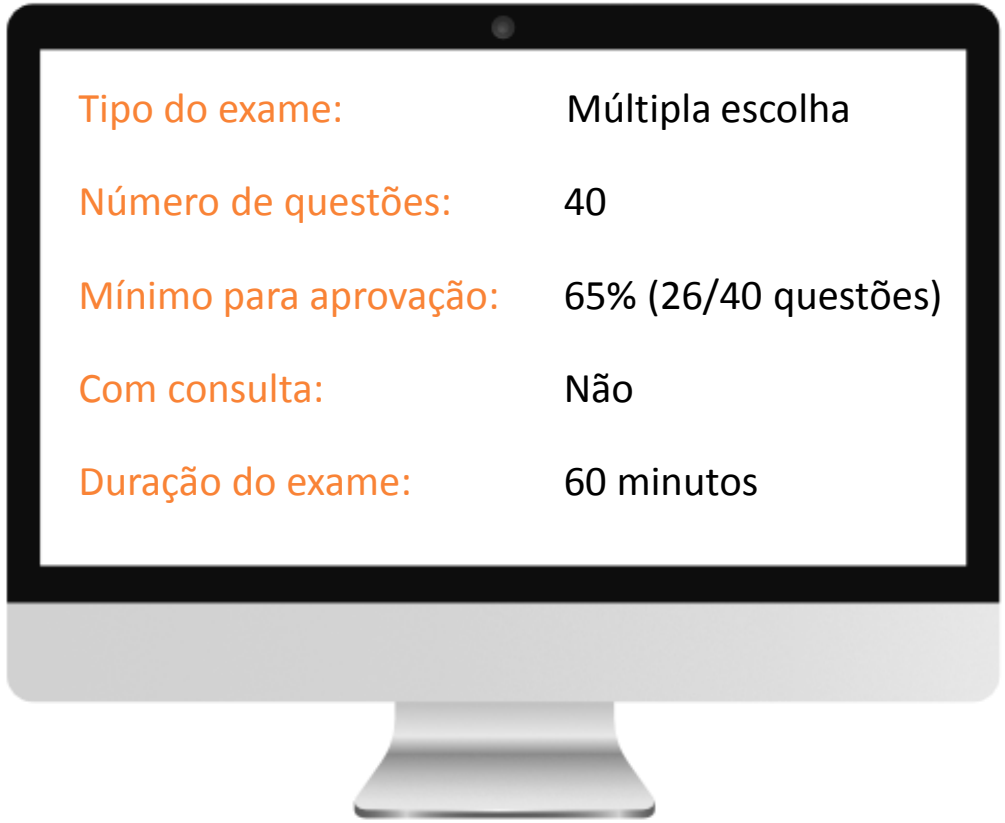
- ✓ Qualquer pessoa na organização que manuseie informações.
- ✓ Proprietários de pequenas empresas a quem alguns conceitos básicos de Segurança da Informação são necessários.
- ✓ Quem deseje iniciar-se como profissional de segurança da informação.

O EXAME

EXIN Information Security Foundation (ISFS)

é uma certificação que valida o conhecimento de um profissional sobre:

- Informação e Segurança: os conceitos, o valor da informação e da importância da confiabilidade.
- Ameaças e Riscos: a relação entre as ameaças e confiabilidade.
- Abordagem e Organização: a política de segurança e estabelecimento da Segurança da Informação.
- Medidas: física, técnica e organizacional.
- Legislação e Regulamentação: a importância e funcionamento.



BIBLIOGRAFIA INDICADA

Fundamentos de Segurança da Informação: com base na ISO 27001 e ISO 27002

Hintzbergen, J., Hintzbergen, K., Smulders, A. e Baars, H.
Brasport, 1ª edição, 2018
ISBN 9788574528601

PORTAL DO TREINAMENTO!

AGENDA

- Informação e Segurança
- Ameaças e Riscos
- Abordagem e Organização
- Medidas
- Legislação e regulamentos

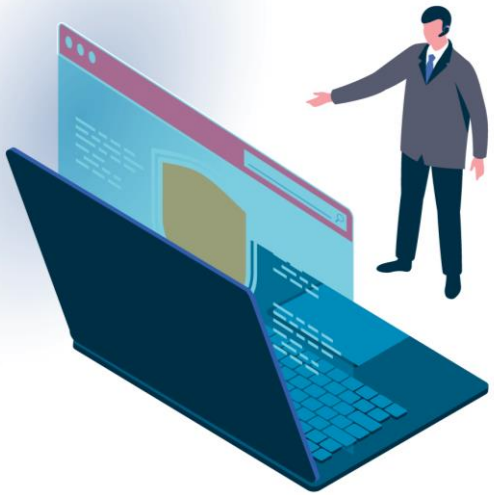
1. Informação e Segurança

1. Informação e Segurança

Tópicos

- Introdução
- O conceito de informação
- Valor da informação
- Aspectos de Confiabilidade

1.1 INTRODUÇÃO



SEGURANÇA DA INFORMAÇÃO

Segurança da informação é preservação da confidencialidade, integridade e disponibilidade da informação.

A partir desta definição podemos dizer que a segurança da informação é a proteção da informação contra uma ampla gama de ameaças, a fim de garantir a continuidade dos negócios, minimizar os riscos de negócio e maximizar o retorno sobre os investimentos e as oportunidades de negócio.

Outras propriedades, tais como autenticidade, responsabilidade, não repúdio e confiabilidade, podem ser incluídas.

SEGURANÇA DA INFORMAÇÃO

A segurança da informação é o caminho para encontrar o equilíbrio correto entre diversos aspectos:

- Os requisitos de qualidade que uma organização pode ter para a sua informação.
- Os riscos associados a esses requisitos de qualidade.
- As contramedidas que são necessárias para mitigar esses riscos.
- A garantia da continuidade do negócio em caso de um desastre.
- Se e quando relatar incidentes fora da organização.

SEGURANÇA DA INFORMAÇÃO

A segurança da informação pode ser obtida através da implantação de um **conjunto adequado de controles,** que pode incluir :

- Políticas,
- Procedimentos,
- Estrutura organizacional
- Funções de hardware e software

Os quais devem ser estudados **e analisados para cada caso**, uma vez que **toda organização é única e possui sua própria necessidades e exigências**.

NORMAS ISO 27000

A família de Normas ISO 27000 é um conjunto de normas que tratam do tema segurança da informação, em seus vários aspectos. É um conjunto extenso com mais de quarenta normas , onde destacamos :

Norma	Tema
ISO/IEC 27000	SGSI – Visão Geral e Vocabulário
ISO/IEC 27001 Sistemas de gestão de segurança da informação - Requisitos	Fornecer os requisitos para estabelecer, implementar, operar, monitorar, revisar, manter e melhorar um Sistema de Gestão de Segurança da Informação (SGSI)
ISO/IEC 27002 Código de prática para controles de segurança da informação (Código de boas práticas de segurança da informação)	Fornece diretrizes para padrões de segurança da informação organizacional e práticas de gerenciamento de segurança da informação, incluindo a seleção, implementação e gerenciamento de controles levando em consideração o (s) ambiente (s) de risco de segurança da informação da organização.

NORMAS ISO 27000

Norma	Tema
ISO/IEC 27003 Sistemas de gestão de segurança da informação - Orientação	Descreve o processo de especificação do projeto do SGSI desde a concepção até a elaboração dos planos de implantação, obtenção da aprovação da direção para implementar o SGSI.
ISO/IEC 27004 Gestão da segurança da informação - Monitoramento, medição, análise e avaliação	Fornece diretrizes destinadas a auxiliar as organizações na avaliação do desempenho da segurança da informação e da eficácia de um sistema de gestão da segurança da informação, a fim de cumprir os requisitos da ISO/IEC 27001
ISO/IEC 27005 Gerenciamento de riscos de segurança da informação	Fornece diretrizes para o gerenciamento de riscos de segurança da informação. Apoia os conceitos gerais especificados na ISO/IEC 27001 e é projetado para auxiliar na implementação satisfatória da segurança da informação com base em uma abordagem de gerenciamento de risco.

FATORES CRÍTICOS DE SUCESSO

A implantação com sucesso de segurança de informação em uma organização passa por alguns pontos de atenção, conforme a norma ISO/IEC 27001.

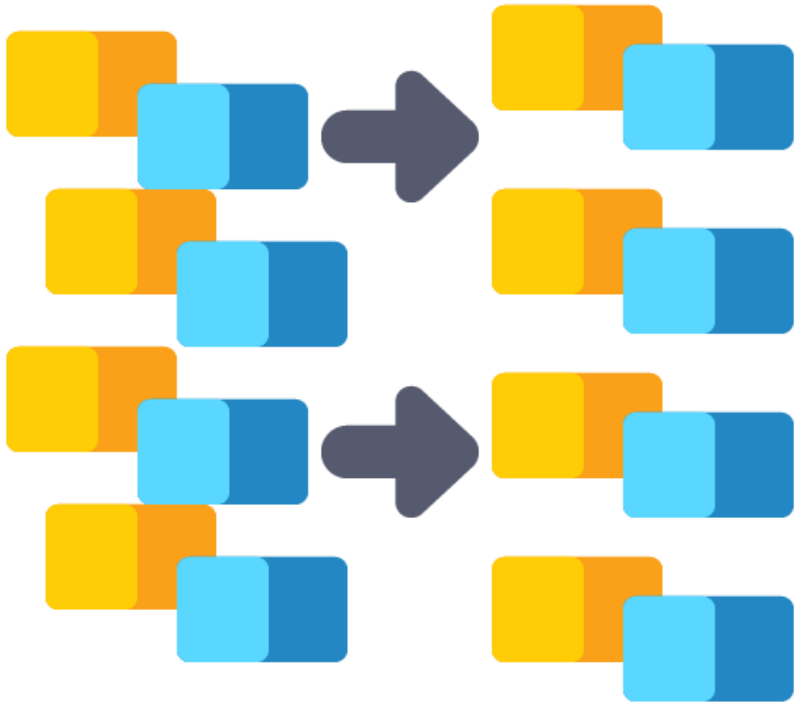
- Política de Segurança da Informação refletindo os objetivos do negócio.
- Foco de implementação consistente com a cultura organizacional.
- Comprometimento e apoio visível da direção.
- Bom entendimento dos requisitos de segurança, avaliação e gerenciamento de riscos.

FATORES CRÍTICOS DE SUCESSO

Continuação

- Divulgação eficiente da segurança para todos os colaboradores.
- Distribuição das diretrizes sobre as normas e política da segurança da informação para todos os funcionários, clientes e fornecedores.
- Proporcionar educação e treinamentos adequados.
- Um sistema de medição abrangente utilizado para avaliar o desempenho da gestão da segurança da informação e obtenção de sugestões para a melhoria

1.2 CONCEITOS DE INFORMAÇÃO



DADO e INFORMAÇÃO

DADO

Os dados são uma coleção de fatos, como números, palavras, medidas, observações ou apenas descrições de coisas.

INFORMAÇÃO

Informação é o resultado do processamento, tratamento e organização de dados, de tal forma que represente uma modificação no conhecimento do sistema (Humano ou Máquina) que a recebe.

Informação é o dado que tem significado em algum contexto para quem o recebe.

FORMATOS E MEIOS DA INFORMAÇÃO

A informação está **presente em vários formatos e meios** (mídias) :

Textos - em documentos físicos, documentos digitais

Imagens – Fotografias analógicas ou digitais , captadas por câmeras de segurança, etc

Verbal - conversas , gravações , transmitidas por rádio ou televisão, etc.

1.3 O VALOR DA INFORMAÇÃO

O VALOR DA INFORMAÇÃO

Informação é conhecimento que alguém tenha adquirido.

O valor que este conhecimento possa ter, varia de pessoa para pessoa. Enquanto alguns podem considerar este conhecimento desinteressante, outros podem ser capazes de extrair informações valiosas a partir dele.

O valor da informação é, portanto, **determinado pelo valor que o usuário lhe atribui.**

INFORMAÇÃO COMO FATOR DE PRODUÇÃO

Capital, trabalho e matérias primas, são normalmente considerados fatores de produção de uma empresa ou organização.

Para tecnologia da informação, é comum considerar a informação como fator de produção, considerando que organizações e empresas não podem existir sem informação.

GERENCIAMENTO DA INFORMAÇÃO

A **forma como uma organização trata suas informações** e garante que o valor da informação seja identificado e explorado em toda a sua extensão. Independentemente de sua forma (papel, digital, etc) .

- planeja,
- coleta,
- organiza,
- utiliza,
- controla,
- dissemina,
- descarta.

SISTEMAS DE INFORMAÇÃO

Dentro deste contexto, a **infraestrutura de tecnologia da informação vem ganhando cada vez mais importância em como tratamos e acessamos a informação**, o que inclui:

- Desktop / Notebook
- Rede, cabeada ou sem fio
- Servidores
- Armazenamento de dados
- Telefones móveis
- Rede móvel e/ou Bluetooth

1.4 ASPECTOS DE CONFIABILIDADE

CONFIABILIDADE DA INFORMAÇÃO

Para proteger o valor da informação e manter sua confiabilidade, devem ser analisado os três requisitos de qualidade da informação :

- Confidencialidade
- Integridade
- Disponibilidade

C I D

CONFIDENCIALIDADE

CONFIDENCIALIDADE

Propriedade em que a informação não é disponibilizada ou divulgada para pessoas, entidades ou processos não autorizados.

Características:

Exclusividade – Os dados só estarão disponíveis para os usuários autorizados a acessá-los;

Privacidade –Aplicação do conceito de exclusividade, de forma que os dados armazenados no sistema não sejam acessados por outros usuários.

CONFIDENCIALIDADE

Medidas de confidencialidade

- Criptografia de Dados
- Estrito controle de acesso Físico e Lógico - Assegurar o nível de acesso apropriado e somente para as pessoas autorizadas
- Classificação de dados – Definir a que publico os dados podem ser comunicados . Públicos ? Sensíveis? Confidenciais ?
- Treinamento de pessoal
- Segregação de Funções – Evitar que funções conflitantes sejam executadas pela mesma pessoa
- Política de Mesa Limpa - Manter documentos confidenciais em locais seguros

INTEGRIDADE

INTEGRIDADE

A integridade se refere a ser correto e consistente com o estado ou a informação pretendida

(completude / completeza e exatidão)

São características:

Autenticidade - Certeza de que uma informação pertence ao autor declarado.

Não repúdio - Impossibilidade de negar responsabilidade sobre seus atos.

Auditabilidade - Grau de facilidade com que podemos checar a origem e consistência das informações.

INTEGRIDADE

Medidas de integridade

- Técnicas de criptografia – Protege a informação de acesso ou mudança não autorizada.
- Gravação de logs de usuários – Garantir que possa ser determinado quem modificou a informação.
- Segregação de Função, posições e autoridade : Ao menos duas pessoas serão necessárias para realizar mudanças que tenham graves consequências.
- Mudanças em sistemas e dados devem ser são autorizadas.
- Onde possível, são criados mecanismos que forcem as pessoas a usar o termo correto. por exemplo, um incidente é sempre chamado de “incidente”; o termo “chamado” não pode ser inserido na base de dados.

DISPONIBILIDADE

DISPONIBILIDADE

Propriedade de ser acessível e utilizável sob demanda por uma entidade autorizada.

São características:

Oportunidade - a informação está disponível quando necessário.

Continuidade - os usuários conseguem continuar trabalhando no caso de falha.

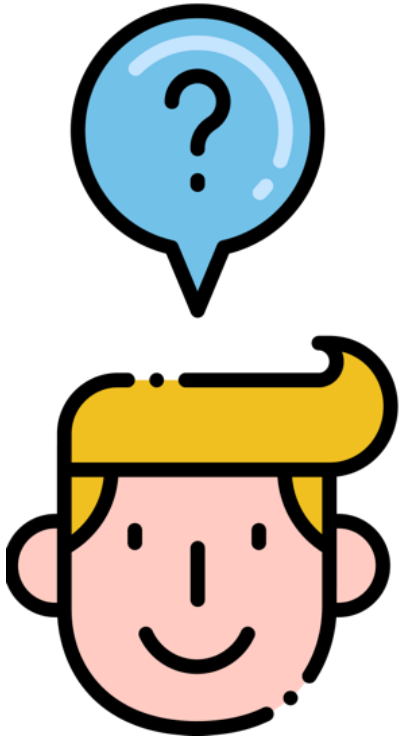
Robustez - existe capacidade suficiente para permitir que todos os usuários trabalhem no sistema.

DISPONIBILIDADE

Medidas de disponibilidade

- Gestão back-up e restore robusto
- Não armazenar dados em máquinas pessoais, dar preferência a sistemas de armazenamento centralizados, como servidores em rede interna ou cloud.
- Cumprir requisitos legais sobre armazenamento de dados

1.5 EXERCÍCIOS



EXERCÍCIOS

1. O que é dado ? e Informação ?

   Os dados são uma coleção de fatos, como números, palavras, medidas, observações ou apenas descrições de coisas.

   Informação é o dado que tem significado em algum contexto para quem o recebe.

2. Defina Segurança da Informação .

   Segurança da informação é preservação da confidencialidade, integridade e disponibilidade da informação.

EXERCÍCIOS

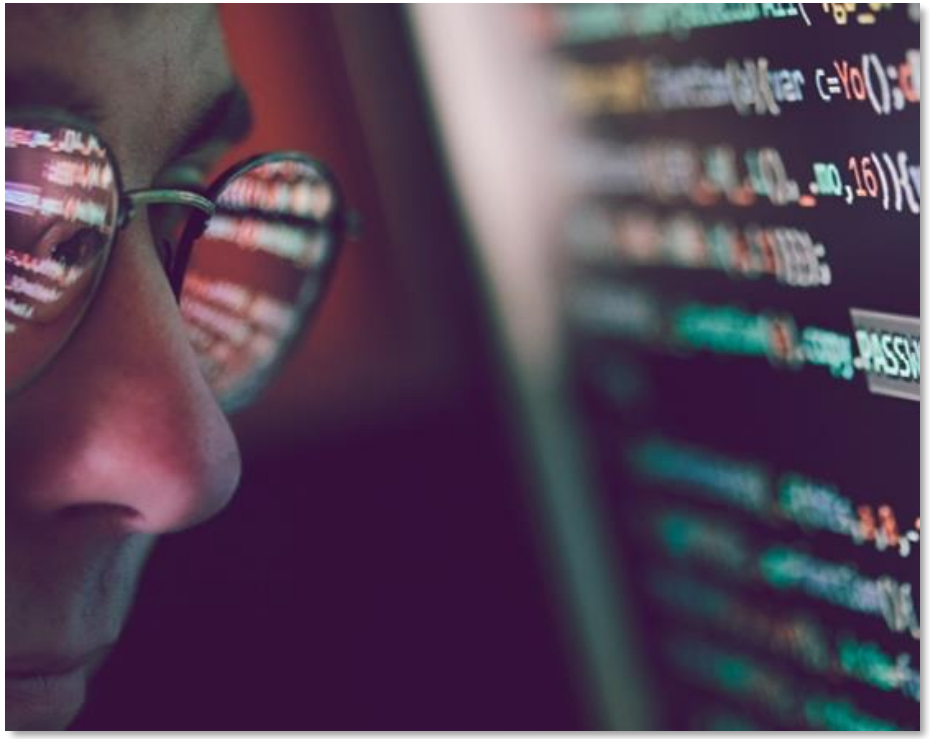
3. Quais são os aspectos da confiabilidade de Informação

Confidencialidade
Integridade
Disponilidade

4. O que é Gerenciamento da Informação ?

A **forma como uma organização trata suas informações** e garante que o valor da informação seja identificado e explorado em toda a sua extensão. Independentemente de sua forma (papel, digital, etc)

2. Ameaças e Riscos



2. Ameaças e Riscos

Tópicos

- Ameaças e Riscos
- Gerenciamento de Risco
- Tipo de Ameaças
- Tipo de Danos

2.1 AMEAÇAS E RISCOS

Ameaças e Riscos

Definições

- **Ativo**: Qualquer coisa que tenha valor para a organização.
  Por exemplo : Instalações, informações, software, equipamentos, pessoas, habilidades, conhecimentos, etc.
- **Vulnerabilidade**: Fraqueza de um ativo ou controle (medida de segurança) que pode ser explorada por uma ou mais ameaças .
- **Ameaça**: Causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema ou organização.
- **Medidas ou Controles de segurança** – Ações realizadas para proteger um sistema de informação contra ataques à “CID”. Sinônimos: proteção, salvaguarda e contramedida.

Ameaças e Risco

Definições

- **Risco**: Efeito da incerteza sobre os objetivos. Risco à segurança da informação está associado à probabilidade de ameaças explorarem vulnerabilidades de um ativo de informação e causar danos a uma organização.

2.2 GERENCIAMENTO DE RISCO

GERENCIAMENTO DE RISCO

- Gerenciamento de riscos é o processo de planejar, organizar, conduzir e controlar as atividades de uma organização visando minimizar os efeitos do risco sobre o capital e o lucro de uma organização.

- É um processo contínuo a ser aplicado a todos os aspectos dos processos operacionais no qual os riscos são identificados, examinados e reduzidos a um nível aceitável.

ANÁLISE DE RISCO

Uma análise de riscos ajuda a empresa a avaliar corretamente os riscos e a estabelecer medidas de segurança corretas e equilibradas.

O objetivo de realizar uma análise de riscos é :

- Identificar quais ameaças são relevantes para os processos operacionais
- Identificar os riscos associados.
- Definir o nível de segurança apropriado
- Definir medidas de segurança

ANÁLISE DE RISCO

Uma análise de riscos possui quatro objetivos principais:

- Identificar os ativos e seus valores.
- Determinar as vulnerabilidades e ameaças.
- Determinar o risco de as ameaças se tornarem realidade e interromperem os processos operacionais.
- Estabelecer um equilíbrio entre os custos de um incidente e os custos de uma medida de segurança.

ANÁLISE DE RISCO

Há dois tipos principais de análises de riscos:

- Análise quantitativa do risco.
- Análise qualitativa do risco.

ESTRATÉGIA DE RISCO

Podemos lidar com os riscos de diferentes formas, porem, independente da estratégia escolhida, a administração tem que tomar uma decisão consciente e assumir as consequências.

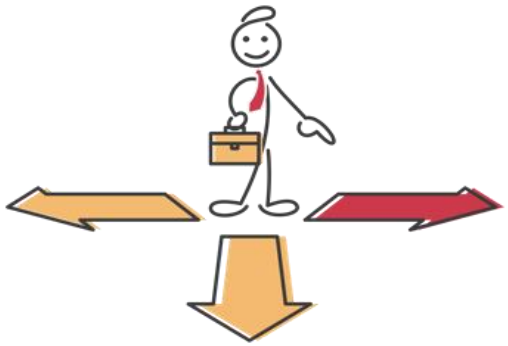
Estratégias de Risco

Reter Riscos - Retenção ou tolerância a riscos significa que certos riscos são aceitos

Redução (ou mitigação) do risco - Medidas de segurança são realizadas para que as ameaças : não mais se manifestem, ou se ocorrer, o dano resultante é minimizado.

Prevenção do risco (Evitar Riscos) - Medidas são tomadas para que a ameaça seja neutralizada

Transferir risco – Transfere o impacto de uma ameaça para terceiros juntamente com a propriedade da resposta.



2.3 TIPOS DE AMEAÇAS

TIPOS DE AMEAÇAS

- Para se proteger é necessário saber reconhecer uma ameaça.

- Para determinar as ameaças, profissionais de segurança da informação utilizam listas padrões de ameaças como a ISO/IEC 27005

Ameaças podem ser divididas em:

- Ameaças humanas
- Ameaças não humanas

TIPOS DE AMEAÇAS

Ameaças humanas

Ameaça humana intencional

As pessoas podem intencionalmente causar danos a sistemas de informação por várias razões.

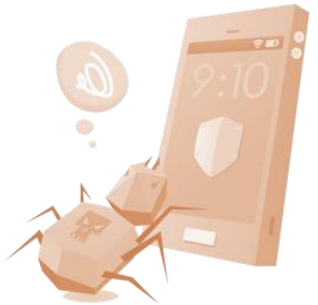
- ameaças externas como um hacker
- funcionário da empresa que destrói ou vende dados após ser demitido ou, como resultado de não receber a promoção
- situações estressantes podem levar colaboradores irritados a reagir excessivamente em algumas ocasiões
- técnicas de engenharia social tira proveito dos pontos fracos das pessoas para concretizar seus objetivos

TIPOS DE AMEAÇAS

Ameaças humanas

Ameaça humana não intencional

As pessoas também podem causar danos de forma não intencional. Por exemplo :



- pressionando acidentalmente o botão “Delete” e confirmando com OK.
- inserir um pen drive, ou instalar um software com vírus em uma máquina e espalhar o vírus através da rede.
- em pânico, usar um extintor de pó para apagar um pequeno incêndio e, como resultado, destruir um servidor.

TIPOS DE AMEAÇAS

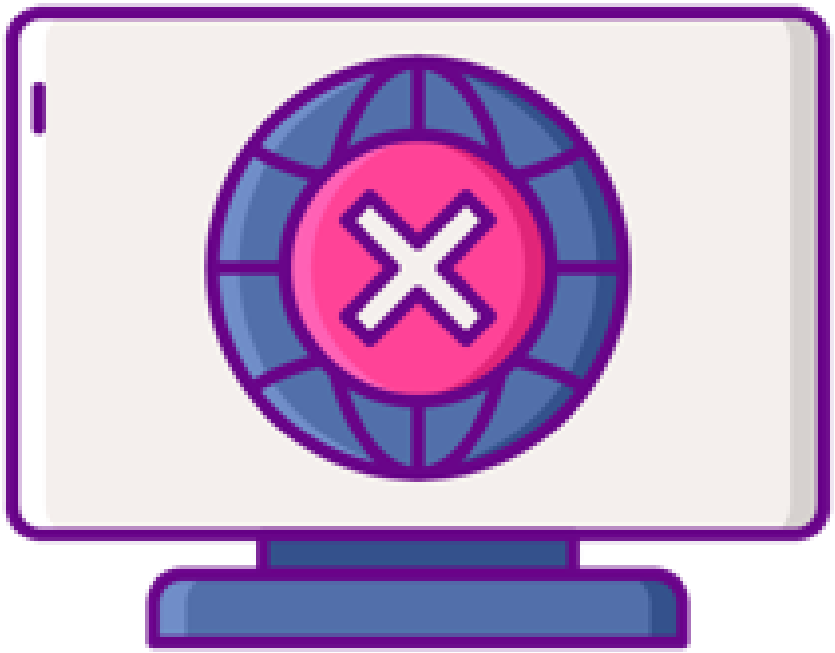
Ameaças não humanas

Existem eventos não humanos que ameaçam uma organização.

- **De fontes externas :**
  - Raios, incêndios, inundações, terremotos, tempestades.

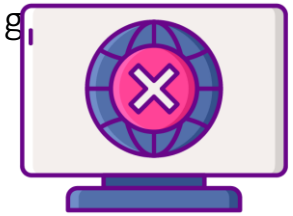
- **De fontes internas** :
  - A sala do servidor está localizada sob um telhado plano suscetível a vazamento?
  - Situada no subsolo em uma área onde há água subterrânea elevada?

2.4 TIPOS DE DANO (OU IMPACTO)



TIPOS DE DANO (OU IMPACTO)

Danos são os resultados da ocorrência de uma ou mais ameaças, e podem ser classificados em dois g



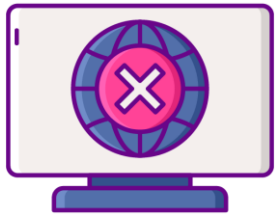
Danos diretos

Prejuízo direto ao negócio

Exemplos

- Furto
- Causado pelo fogo em um incêndio
- Causado pelo material do extintor de incêndio, por exemplo água em um servidor

TIPOS DE DANO (OU IMPACTO)



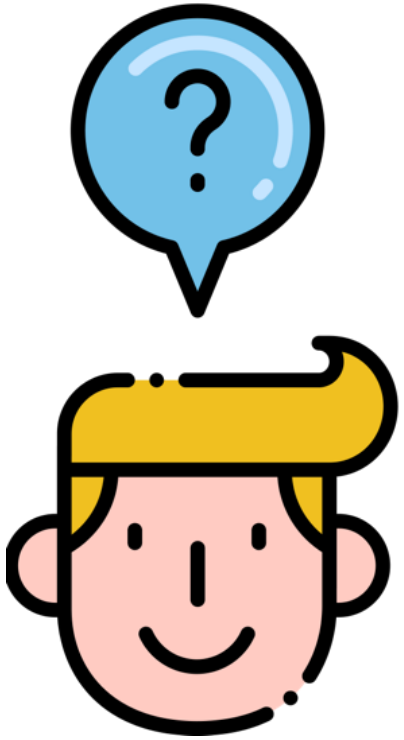
Danos indiretos

Dano indireto é a perda consequente do que ocorreu.

Exemplos

- ser incapaz de atender a um contrato devido à infraestrutura de TI ter sido destruída pelo incêndio
- Queda do site de e-commerce devido a um ataque hacker ao servidor.

2.5 EXERCÍCIOS



EXERCÍCIOS

1. Definir Ameaça e Risco

Ameaça: Causa potencial de um incidente indesejado, a qual pode resultar no dano a um sistema ou organização.

Risco: Efeito da incerteza sobre os objetivos.

2. O que é dano Direto e Indireto . Forneça exemplos.

Danos diretos

Prejuízo direto ao negócio

Exemplos

- Furto
- Causado pelo fogo em um incêndio
- Causado pelo material do extintor de incêndio, por exemplo água em um servidor

Danos indireto: Dano indireto é a perda consequente do que ocorreu.

Exemplos

- ser incapaz de atender a um contrato devido à infraestrutura de TI ter sido destruída pelo incêndio
- Queda do site de e-commerce devido a um ataque hacker ao servidor.

EXERCÍCIOS

3. Quais são os métodos de análise de risco . Descreva-os

Há dois tipos principais de análises de riscos:

- Análise quantitativa do risco : baseada em fatos/números
- Análise qualitativa do risco : baseada em cenários

4. Quais são as principais estratégias de risco ?

- Reter Riscos
- Redução (ou mitigação) do risco
- Prevenção do risco (Evitar Riscos)
- Transferir risco

3. Abordagem e Organização

3. Abordagem e Organização

Tópicos

- Política de Segurança e Organização de Segurança
- Componentes da Organização da Segurança
- Gerenciamento de Incidentes

3.1 POLÍTICA E ORGANIZAÇÃO

POLÍTICA DE SEGURANÇA

Política - A intenção e orientação geral formalmente expressa pela administração.

Política para a segurança da informação - provê as diretivas e o apoio para a organização no que diz respeito a segurança da informação, e :

- Deve ser escrita em conformidade com os requisitos do negócio, bem como com as leis e os regulamentos .
- Deve ser aprovada pela alta direção da empresa e/ou seu conselho de administração e divulgada para todo o seu pessoal e todos os parceiros externos relevantes, tais como clientes e fornecedores.
- Deve haver um programa de conscientização de forma a garantir que todos os colaboradores conheçam a política de segurança.
- Deve ser definido um responsável, que tenha responsabilidade gerencial aprovada para o desenvolvimento, a revisão e a avaliação de política.

ORGANIZAÇÃO DA SEGURANÇA

A implantação da Política de Segurança e garantia que está sendo cumprida na organização, é o estágio seguinte à definição da política em si, e para tal , muitas organizações utilizam o **Ciclo PDCA – Plan-Do-Check-Act** em conjunto com a norma **ISO/IEC 27001** (SGSI – Sistema de Gerenciamento de Segurança da Informação)

Modelo P D C A

O modelo PDCA ou Ciclo de Deming, é utilizado como base para determinar, implementar, monitorar, controlar e manter o Sistema de Gestão da Segurança da Informação (SGSI)

- Planejar (Estabelecer o SGSI): Na fase de estabelecimento, a Política de Segurança da Informação é desenvolvida e documentada
- Implementar e Operar (Implantar o SGSI): Nessa fase, a política da segurança, os documentos relacionados e medidas de segurança são implementadas
- Checar (Monitorar e Verificar o SGSI): Nessa fase, os controles são realizados utilizando a auto avaliação (auditoria interna) e medições são realizadas
- Agir (Manter e Melhorar o SGSI): Nessa fase, as correções são realizadas e as medidas preventivas são tomadas

Sistema de Gerenciamento da Segurança de Informação

A.5 Políticas de segurança da informação;
A.6 Organização da segurança da informação;
A.7 Segurança em recursos humanos;
A.8 Gestão de ativos;
A.9 Controle de acesso;
A.10 Criptografia;
A.11 Segurança física e do ambiente;
A.12 Segurança das operações;
A.13 Segurança nas comunicações;
A.14 Aquisição, desenvolvimento e manutenção de sistemas;
A.15 Relacionamento na cadeia de suprimento;
A.16 Gestão de incidentes de segurança da informação;
A.17 Aspectos de segurança da informação na gestão de continuidade de negócio
A.18 Conformidade.

ISO 27001

ISO 27001- Anexo A

14 seções, 35 objetivos de controle e 114 controles

A.5 Políticas de segurança da informação – controles sobre como as políticas são escritas e revisadas
A.6 Organização da segurança da informação – controles sobre como as responsabilidades são designadas; inclui controles para dispositivos móveis e trabalho remoto
A.7 Segurança em recursos humanos – controles para antes da contratação, durante e após a contratação
A.8 Gestão de ativos – controles relacionados ao inventário de ativos e uso aceitável, e também para a classificação de informação e manuseio de mídias
A.9 Controle de acesso – controles para a política de controle de acesso, gestão de acesso de usuários, controle de acesso a sistemas e aplicações, e responsabilidades dos usuários
A.10 Criptografia – controles relacionados a gestão de chaves criptográficas
A.11 Segurança física e do ambiente – controles definindo áreas seguras, controles de entrada, proteção contra ameaças, segurança de equipamentos, descarte seguro, política de mesa limpa e tela limpa, etc.
A.12 Segurança nas operações – vários controles relacionados a gestão da produção de TI: gestão de mudança, gestão de capacidade, software malicioso, cópia de segurança, registro de eventos, monitoramento, instalação, vulnerabilidades, etc.

PORTAL DO TREINAMENTO!

ISO 27001- Anexo A

14 seções, 35 objetivos de controle e 114 controles

A.13 Segurança nas comunicações – controles relacionados a segurança em rede, segregação, serviços de rede, transferência de informação, mensageria, etc.
A.14 Aquisição, desenvolvimento e manutenção de sistemas – controles definindo requisitos de segurança e segurança em processos de desenvolvimento e suporte
A.15 Relacionamento na cadeia de suprimento – controles sobre o que incluir em acordos e como monitorar os fornecedores
A.16 Gestão de incidentes de segurança da informação – controles para reportar eventos e fraquezas, definindo responsabilidades, procedimentos de resposta e coleta de evidências
A.17 Aspectos da segurança da informação na gestão da continuidade do negócio – controles requisitando o planejamento da continuidade do negócio, procedimentos, verificação e revisão e redundância da TI
A.18 Conformidade – controles requisitando a identificação de leis e regulamentações aplicáveis, proteção da propriedade intelectual, proteção de dados pessoais e revisões da segurança da informação

ISO 27001- Anexo A

14 seções, 35 objetivos de controle e 114 controles

A.13 Segurança nas comunicações – controles relacionados a segurança em rede, segregação, serviços de rede, transferência de informação, mensageria, etc.
A.14 Aquisição, desenvolvimento e manutenção de sistemas – controles definindo requisitos de segurança e segurança em processos de desenvolvimento e suporte

A.14.2.7 Desenvolvimento terceirizado: pode ser marcado como não aplicável, caso uma organização não terceirize o desenvolvimento de software

A.15 Relacionamento na cadeia de suprimento – controles sobre o que incluir em acordos e como monitorar os fornecedores
A.16 Gestão de incidentes de segurança da informação – controles para reportar eventos e fraquezas, definindo responsabilidades, procedimentos de resposta e coleta de evidências
A.17 Aspectos da segurança da informação na gestão da continuidade do negócio – controles requisitando o planejamento da continuidade do negócio, procedimentos, verificação e revisão e redundância da TI
A.18 Conformidade – controles requisitando a identificação de leis e regulamentações aplicáveis, proteção da propriedade intelectual, proteção de dados pessoais e revisões da segurança da informação

https://pt.slideshare.net/FabioMartins12/iso-270022013

3.2 COMPONENTES DA ORGANIZAÇÃO DA SEGURANÇA

PAPÉIS E RESPONSABILIDADES DA SEGURANÇA DA INFORMAÇÃO

Dependendo do tamanho da organização, pode haver um conjunto de funções ou posições para as várias responsabilidades de segurança da informação.
Esses papeis podem variar quanto aos títulos que lhes são dados, sendo definidos mais ou menos conforme o que segue:

- Chefe de Segurança da Informação (Chief Information Security Officer – CISO) está no mais alto nível gerencial da organização e desenvolve a estratégia geral de segurança para toda a empresa.
- Encarregado da Segurança da Informação (Information Security Officer – ISO) desenvolve a política de segurança da informação de uma unidade de negócio com base na política da empresa e assegura que ela seja seguida.
- Gerente de Segurança da Informação (Information Security Manager – ISM) desenvolve a política de segurança da informação dentro da organização de TI e assegura que ela seja seguida.

PAPÉIS E RESPONSABILIDADES DA SEGURANÇA DA INFORMAÇÃO

Segregação de Funções: Deveres, atividades e responsabilidades, devem ser segregadas a fim de evitar a possibilidade de alterações não autorizadas ou não intencionais, ou uso indevido dos ativos da organização

Contato com autoridades: Contatos apropriados devem ser mantidos com as autoridades policiais locais, pessoal de apoio de emergência e provedores de serviços. As organizações devem ter procedimentos disponíveis que especifiquem quando e por quem as autoridades devem ser contatadas no caso de acesso indevidos a organização, desastres naturais, falta de energia, etc.

GERENCIAMENTO DE ATIVOS DE NEGÓCIOS

Ativos devem ser classificados a fim de permitir a definição de níveis de segurança necessário a cada um, sendo isto responsabilidade do proprietário.

Cada ativo deve ter um dono e deve ser registrado, contendo ao mínimo :

- O tipo de ativo da empresa.
- O dono.
- A localização.
- O formato.
- A classificação.
- O valor para o negócio.
- O custo inicial
- A idade.
- O custo estimado de reposição

GERENCIANDO OS ATIVOS DE NEGÓCIO - MUDANÇAS

Para assegurar que mudanças não possam ser implantadas de maneira descontrolada, é ainda aconselhável

- Criar ambientes segregados (Desenvolvimento, Teste, Aceite e Produção de Sistemas da Informação)
- Efetuar teste de aceitação do Sistema
- Prever e criar procedimentos para mover o software e sistemas de um ambiente para o outro.

B Y O D

Bring Your Own Device (BYOD), ou “traga o seu próprio dispositivo”, onde as empresas dão ao seu pessoal a possibilidade de usar dispositivos próprios para trabalhar na companhia.

Nesta situação os ativos pessoais (um tablet, laptop ou telefone celular) possuem informações de negócio e essas informações devem ser protegidas.

Deve haver uma política para BYOD na empresa e as informações nos ativos BYOD devem ser protegidas.

3.3 GERENCIAMENTO DE INCIDENTES

GERENCIAMENTO DE INCIDENTES- Conceitos

- Incidente : Uma interrupção não planejada de um serviço ou redução na qualidade de um serviço (ITIL 4)
  - Incidente de Segurança da Informação : Um incidente de segurança é um evento de segurança ou um conjunto deles, confirmado ou sob suspeita de impactar a disponibilidade, integridade, confidencialidade ou a autenticidade de um ativo de informação
    - Evento de segurança da informação : Ocorrência identificada de mudança no estado de um sistema, serviço ou rede que indique uma possível violação da política de segurança da informação ou falha de proteção

GERENCIAMENTO DE INCIDENTES- Conceitos

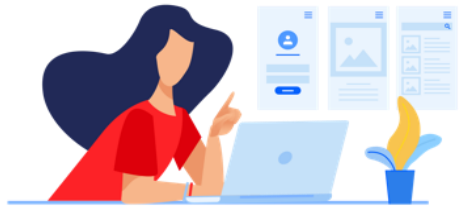
- Gerenciamento de incidentes de segurança da informação
  - Processos para detectar, reportar, avaliar, responder, lidar e aprender com os incidentes de segurança da informação.
  - O propósito de um processo de gerenciamento de incidentes é garantir que os incidentes e as deficiências relacionadas aos sistemas de informação sejam conhecidos, de forma que as medidas apropriadas possam ser tomadas em tempo hábil
  - O padrão ISO/IEC 20000 ou o framework ITIL descrevem como incidentes podem ser geridos no processo de gerenciamento de incidentes.

GERENCIAMENTO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Algumas habilidades básicas são primordiais para o gerenciamento de incidentes em uma organização

Informar : Colaboradores da organização devem ser capazes de **identificar e informar incidentes** o que é um incidente de segurança, como :

- Um documento confidencial foi deixado na impressora.
- Um arquivo com informações pessoais desapareceu.
- Uma porta que deveria estar fechada, está aberta.
- Um colega está se comportando de forma estranha
- A tela do computador apresenta mensagens estranhas.



REPORTANDO INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Informar incidentes de segurança é, principalmente, uma forma de aprender com eles, a fim de evitar que incidentes semelhantes ocorram novamente.

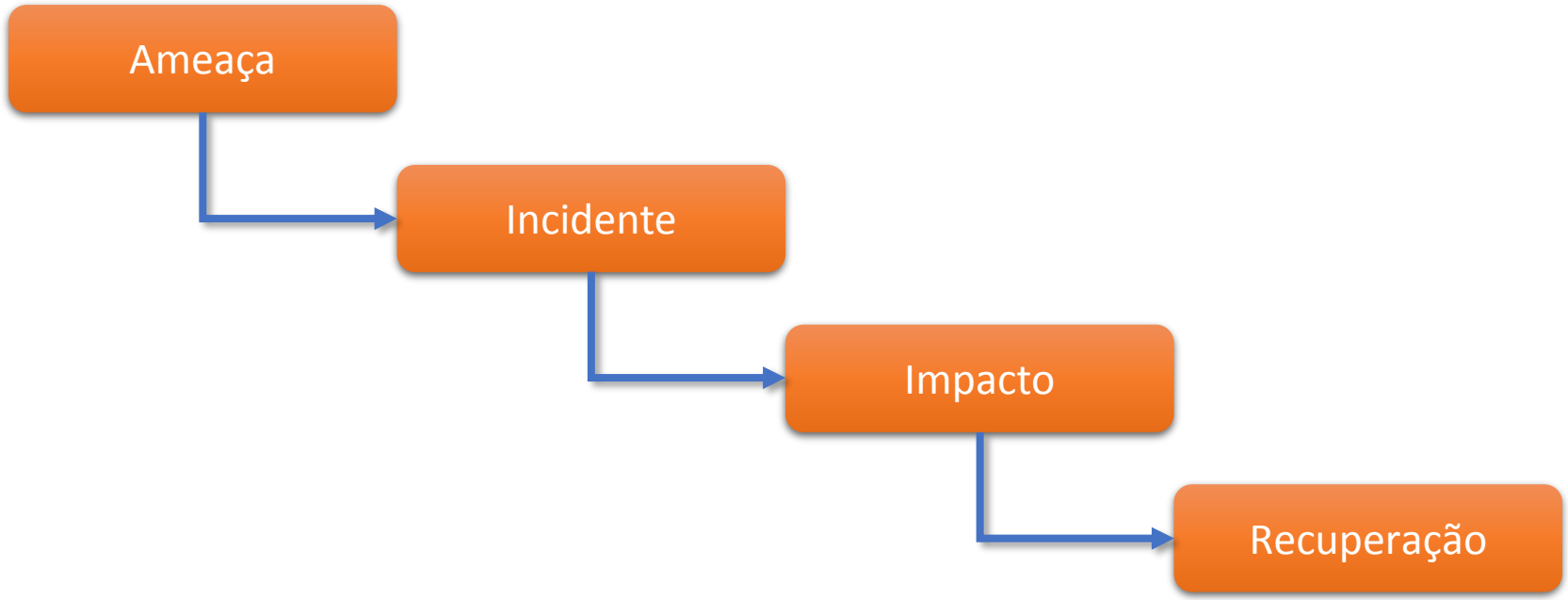
A não notificação de incidentes de segurança pode levar a danos sérios a organização, tanto financeiros, quanto de imagem.

REPORTANDO INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Escalação

- **Escalação funcional (horizontal) :** Se o funcionário da central de atendimento não for capaz de lidar com o incidente (devido a limitação de conhecimento técnico ou falta de autoridade), o incidente pode ser transferido a alguém que possa ser capaz de solucionar o problema.
- **Escalação hierárquica (vertical) :** Um incidente também pode ter que ser reportado a alguém com mais autoridade e que possa tomar uma decisão.

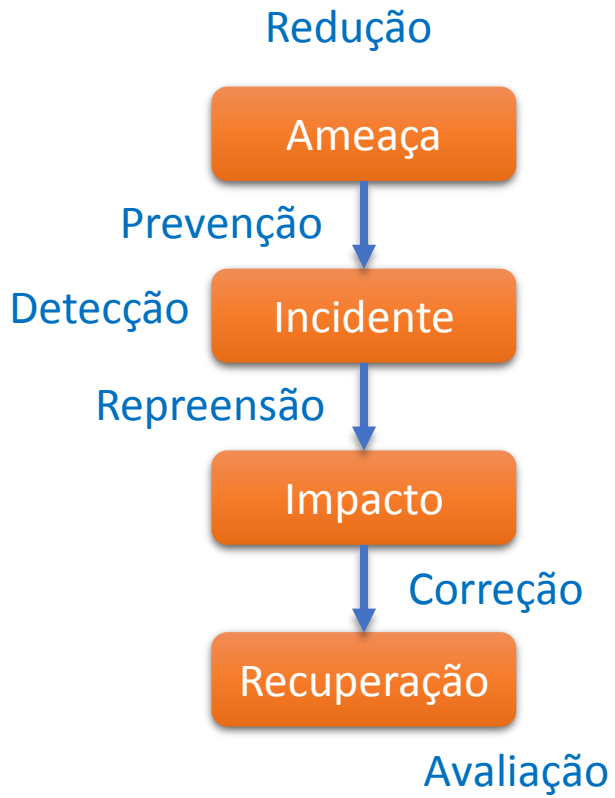
CICLO DO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO



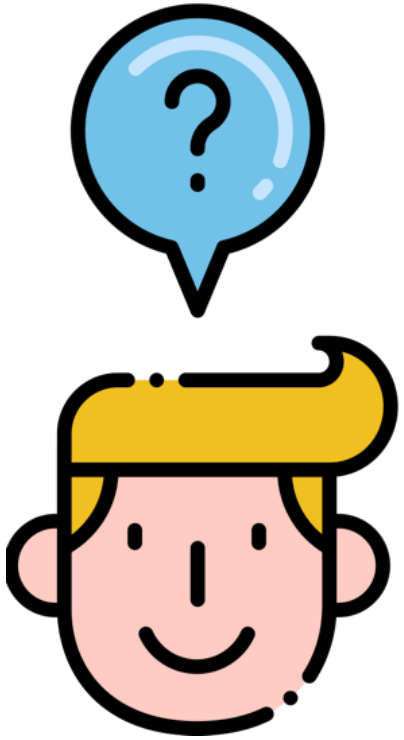
CICLO DO INCIDENTE DE SEGURANÇA DA INFORMAÇÃO

Medidas de segurança atuam em determinado ponto do ciclo de incidentes, e objetivam :

- Reduzir as ameaças (redutiva)
- Prevenir incidentes (preventiva)
- Detectar incidentes (detectiva)
- Parar ameaças / Diminuir impacto (repressiva)
- Corrigir danos (corretiva)
- Entender e evitar nova ocorrência (Avaliar)



3.4 EXERCÍCIOS



EXERCÍCIOS

1. Qual é o objetivo da Política de Segurança da Informação, e quais são seus requisitos ?

A política para a segurança da informação provê as diretivas e o apoio para a organização no que diz respeito a segurança da informação, e :

- Deve ser escrita em conformidade com os requisitos do negócio, bem como com as leis e os regulamentos .
- Deve ser aprovada pela alta direção da empresa e/ou seu conselho de administração e divulgada para todo o seu pessoal e todos os parceiros externos relevantes, tais como clientes e fornecedores.
- Deve haver um programa de conscientização de forma a garantir que todos os colaboradores conheçam a política de segurança.
- Deve ser definido um responsável, que tenha responsabilidade gerencial aprovada para o desenvolvimento, a revisão e a avaliação de política.

EXERCÍCIOS

2. Quais são os tipos de escalação

Funcional ou Horizontal
Hierárquica ou Vertival

3. Qual o objetivo do Gerenciamento de Incidentes de Segurança da Informação

Processos para detectar, reportar, avaliar, responder, lidar e aprender com os incidentes de segurança da informação.

EXERCÍCIOS

4. Quais são a medidas, considerando o ciclo de vida do incidente de segurança

- Reduzir as ameaças (redutiva)
- Prevenir incidentes (preventiva)
- Detectar incidentes (detectiva)
- Parar ameaças / Diminuir impacto (repressiva)
- Corrigir danos (corretiva)
- Entender e evitar nova ocorrência (Avaliar)

5. Qual método utilizado para desenhar, implementar, monitorar e manter o SGSI ?

PDCA

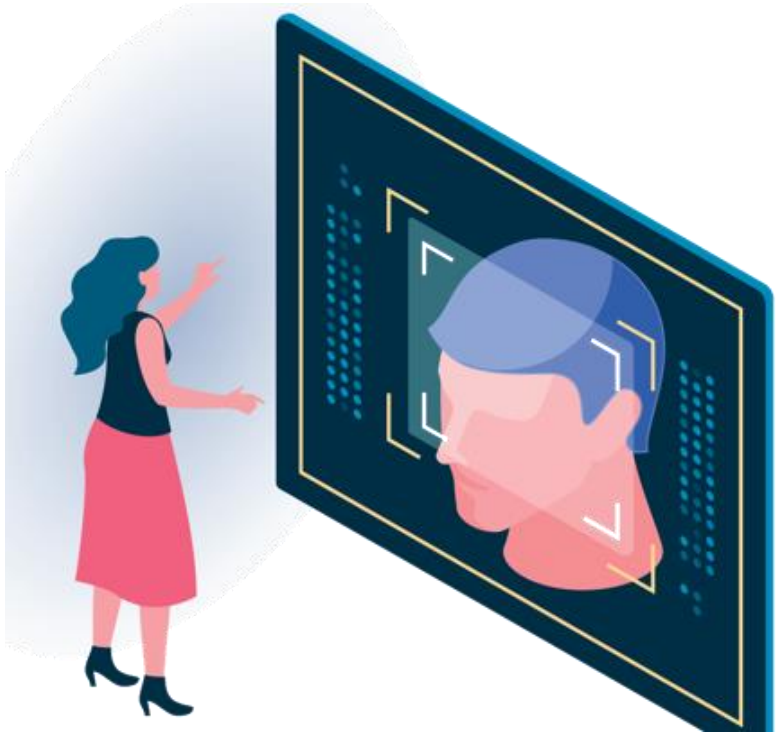
4. Medidas

4. Medidas

Tópicos

- Importância das medidas de segurança
- Medidas Organizacionais
- Medidas Físicas
- Medidas Técnicas

4.1 IMPORTÂNCIA DAS MEDIDAS DE SEGURANÇA

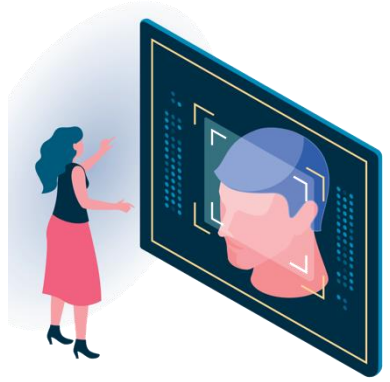


MEDIDAS

Medidas, controles, guardas de segurança e contramedidas são todos termos usados para descrever mecanismos, políticas e procedimentos de segurança, que combatem ataques, reduzem riscos, resolvem vulnerabilidades e melhoram o estado geral de segurança dentro de uma organização

Um bom conjunto de medidas :

- Atenua os aspectos relevantes da CID
- Atua nos três níveis hierárquicos (Estratégico, Tático, Operacional)
- Leva em consideração a proteção lógica (TIC) e a proteção física
- Está incorporado e documentado



CLASSIFICAÇÃO DA INFORMAÇÃO

A classificação é usada para definir diferentes níveis de sensibilidade na qual a informação deve ser estruturada, sendo :

- **Classificar** é o ato de atribuir a classificação apropriada – tal como secreto, confidencial ou público – a uma informação específica.
- **Designar** é uma forma especial de categorizar a informação, por exemplo, de acordo com um determinado assunto da organização ou um grupo de pessoas autorizadas.
- **Dono** é a pessoa encarregada pelo ativo de negócio (Informação).

CLASSIFICAÇÃO DA INFORMAÇÃO

Pública

São informação que pode vir a público sem maiores consequências danosas ao funcionamento normal da organização, e cuja integridade não é vital;

Interna

O acesso a esse tipo de informação deve ser evitado, embora as consequências do uso não autorizado não sejam por demais sérias. Sua integridade é importante, mesmo que não seja vital;

CLASSIFICAÇÃO DA INFORMAÇÃO

Confidencial

Informação restrita aos limites da organização, cuja divulgação ou perda pode levar a desequilíbrio operacional, e eventualmente, perdas financeiras, ou de confiabilidade perante o cliente externo, além de permitir vantagem expressiva ao concorrente;

Secreta

Informação crítica para as atividades da organização, cuja integridade deve ser preservada a qualquer custo e cujo acesso deve ser restrito a um número bastante reduzido de pessoas.

4.2 MEDIDAS ORGANIZACIONAIS

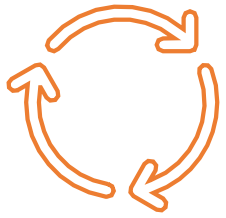
Exemplos de Medidas Organizacionais

- Acordo de confidencialidade / Códigos de conduta
- Descrição de cargos apontando responsabilidades de Segurança da Informação
- Planos e Programas Conscientização de Segurança
- Auditorias
- Regras de acompanhamento / acesso de visitantes
- Gestão de Continuidade de negócio

- Plano de Backups
- Gerenciamento de Mudança
- Segregação de Funções
- Gerenciamento de Terceiros
- Políticas de Guarda, Transporte e Destruição de mídias
- Controle de Acesso

GERENCIAMENTO DA CONTINUIDADE DE NEGÓCIOS

A continuidade diz respeito à disponibilidade dos sistemas de informação no momento em que eles são necessários.



Quais recursos de sua organização precisam estar disponíveis e quando ?

E se ocorrer um desastre, como você irá garantir a continuidade de seus negócios?

GERENCIAMENTO DA CONTINUIDADE DE NEGÓCIOS

O que é um desastre ?

Um evento que impeça a operação normal de sua organização

O objetivo do Gerenciamento de Continuidade de Negócios – GCN (Business Continuity Management – BCM) é

- prevenir que as atividades da organização sejam interrompidas,
- proteger processos críticos das consequências de desastres nos sistemas de informação
- permitir uma rápida recuperação.

GERENCIAMENTO DA CONTINUIDADE DE NEGÓCIOS

Análise de Impacto no Negócio (Business Impact Analysis – BIA)

Tem como objetivo identificar os processos da empresa que são críticos para a operação da organização, identificando as consequências dos desastres e dos incidentes de segurança e as falhas dos serviços,

A partir da BIA , temos :

RTO – Recovery Time Objective - Tempo de Recuperação

RPO – Recovery Point Objective – Ponto de Recuperação

Plano de Continuidade de Negócio

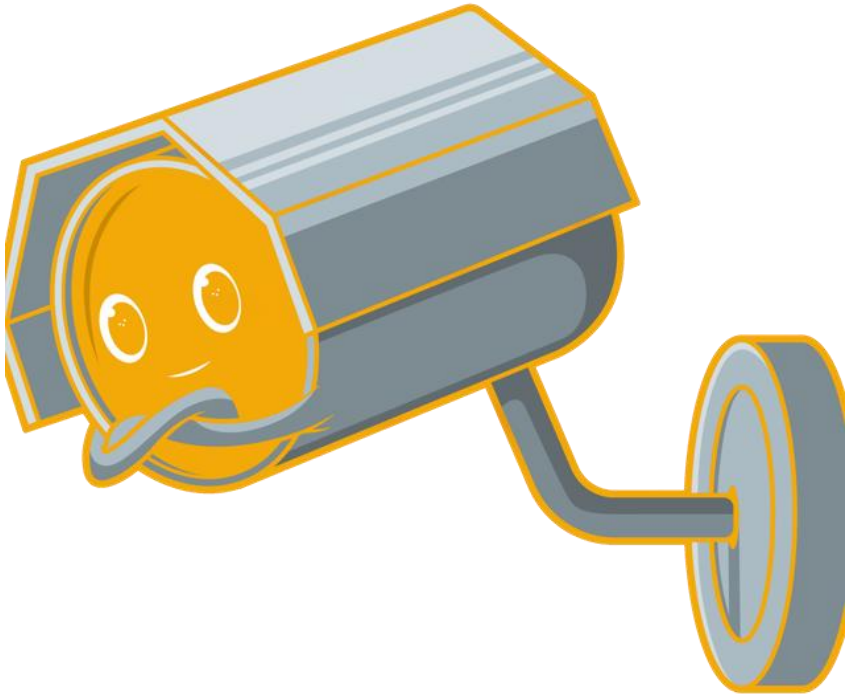
GERENCIAMENTO DA CONTINUIDADE DE NEGÓCIOS

Na segurança da informação, a gestão da continuidade é normalmente dividida em dois componentes separados, porem interligados:

Planejamento de Continuidade do Negócio - PCN (Business Continuity Planning - BCP), onde a continuidade do processo do negócio é garantida. É um conjunto de planos que pode conter:

- PGC – Planos de Gestão de Crises;
- PCO – Planos de Continuidade Operacional;
- PRD – Planos de Recuperação de Desastres - (Disaster Recovery Planning - DRP), onde é organizada a recuperação após um desastre
- PCOM – Planos de Comunicação.

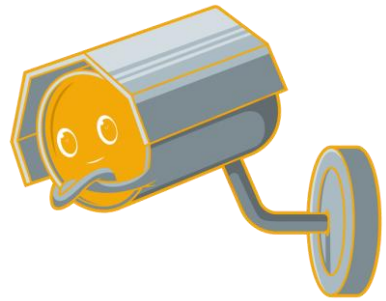
4.3 MEDIDAS FÍSICAS



MEDIDAS FÍSICAS

A segurança física emprega uma combinação de medidas organizacionais, estruturais e técnicas, e precisam ser planejadas e coordenadas de forma interligada. Detectar qualquer invasão é ação comum no tocante a segurança física, a qual usa vários tipos de sensores. Os mais comuns são:

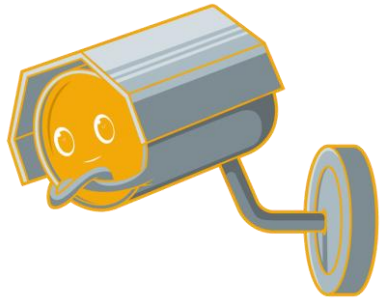
- Detecção passiva por infravermelho
- Câmeras
- Detecção de vibração
- Sensores de quebra de vidro
- Contatos magnéticos



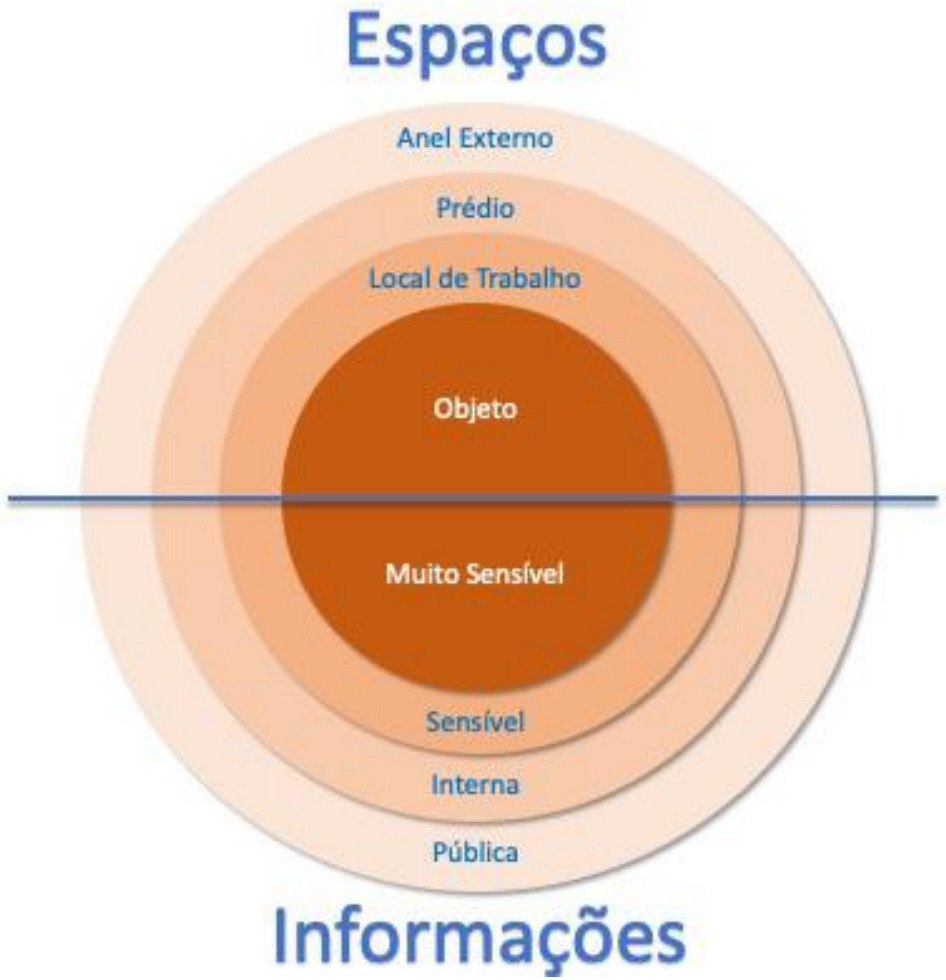
MEDIDAS FÍSICAS

Exemplo de Medidas Físicas

- Equipe de segurança (Vigilantes)
- Correntes / Cadeados
- Algo que faça parte da pessoa (Biometria).
- No-Breaks
- Apagar informações em computadores de colaborar que saiu da empresa
- Algo que a pessoa possua (Documento / Token / Passe)
- Sistema de Câmeras
- Cofres e Armários
- Alarme e sinalização de Incêndios



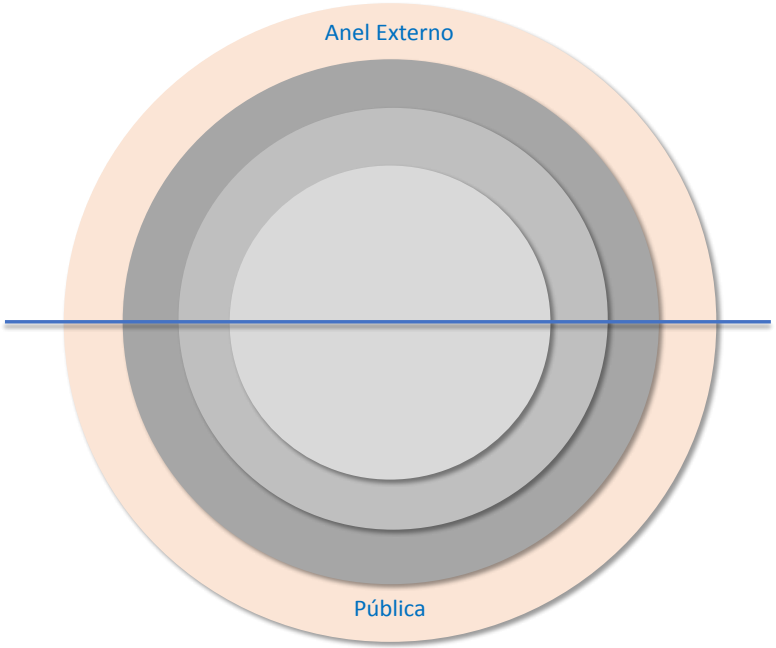
Anéis de Proteção



Anéis de Proteção

Anel externo

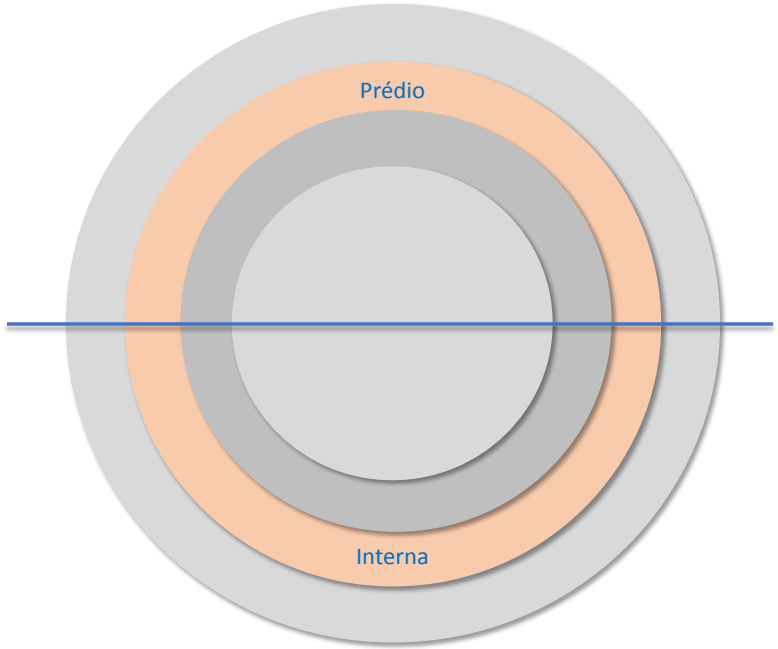
- O anel externo circunda as instalações comerciais pode ser protegido por barreiras naturais e arquitetônicas.
- O anel externo deve permitir o acesso de pessoas autorizadas, portanto, deve ter barreira para verificação eletrônica ou manual.
- A área entre o anel externo e a organização pode ser supervisionada por vigilantes, por serviços auxiliares (manobristas)ou câmeras de vigilância.



Anéis de Proteção

Prédio

Há situações em que não há um anel externo, nestes casos, medidas arquitetônicas como janelas, portas e outros tipos de abertura são importantes. É importante que as medidas de segurança sejam integradas enquanto os prédios estão sendo construídos, já que modificar uma edificação existente pode ser oneroso, e em ambos os casos devem cumprir as legislações pertinentes.

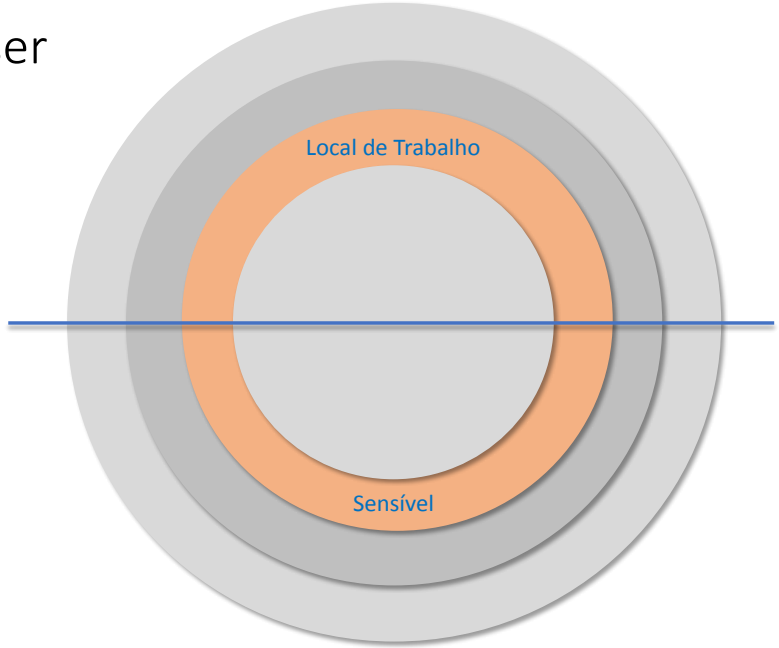


Anéis de Proteção

Local de Trabalho

Cada espaço de trabalho, conforme sua função particular poderá ser objeto de medidas específicas de proteção.

- Detecção de Intrusos
- Salas Especiais
- Não identificação das áreas sensíveis
- Armazenamento de materiais sensíveis e/ou perigosos
- Sala de Servidores:.
- Fitas de Back-up:
- Energia de emergência
- Umidade
- Fogo



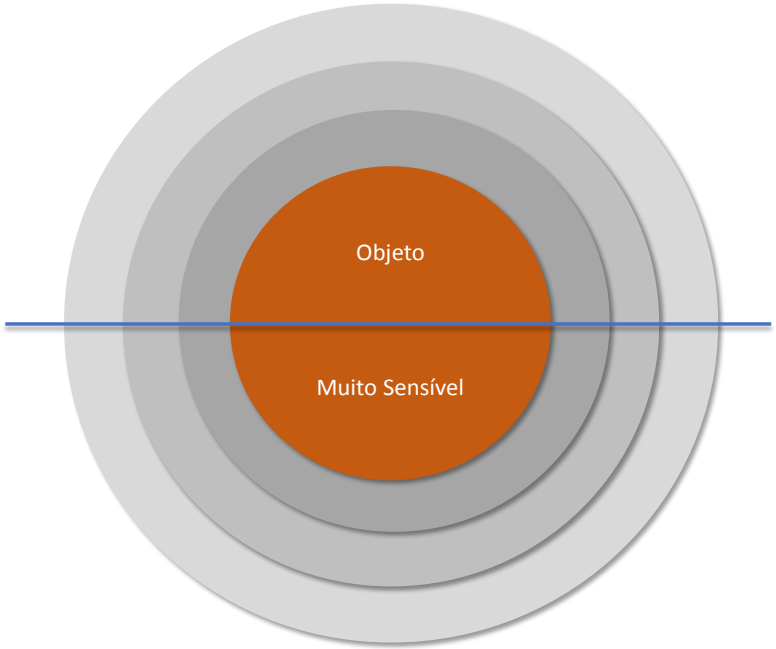
Anéis de Proteção

Objeto

O objeto é a parte mais sensível a ser protegida.

Existem várias opções para segurança de material sensível:

- Armários
- Armários de segurança resistentes ao fogo
- Trava de notebook e monitores
- Salas de acesso restrito



Riscos de falta de segurança física

- Acesso não autorizado
- Exclusão
- Falhas ou indisponibilidade
- Invasão de sistemas
- Roubo
- Sequestro
- Vazamento

4.4 MEDIDAS TÉCNICAS

Medidas Técnicas

O conjunto de medidas técnicas possíveis são extensa, e a escolha de qual ferramenta utilizar vai ser resultado do conhecimento do ambiente a ser protegido e sua sensibilidade a ameaças

EXEMPLOS DE MEDIDAS TÉCNICAS

- Gerenciamento de acesso lógico (perfis , funções)
- Segurança “by Design” – Requisitos de segurança ainda no início do projeto
- Validações de entradas de dados
- Processamento correto dos dados pelas aplicações / sistemas
- Criptografia
- Segurança em dados de testes (dados de testes diferentes dos dados de produção)
- Ações contra vazamentos de informações por canais “invisíveis” (backdoor, porta de manutenção)
- SIEM - Security information and event management

RISCOS RELACIONADOS A SEGURANÇA TÉCNICA

Uma vulnerabilidade técnica é uma fraqueza em um sistema computacional que permite que alguém ataque o sistema computacional vulnerável, por exemplo

- um serviço executando em um servidor
- aplicações ou sistemas operacionais não corrigidos
- acesso discado irrestrito via modem
- porta aberta em um firewall ,
- fraco gerenciamento de senha em servidores e estações de trabalho.

CRIPTOGAFIA, ASSINATURA DIGITAL E CERTIFICADOS

O termo criptografia vem do grego e é uma combinação das palavras "kryptós", que significa "escondido", e "gráphein", que significa "escrita".

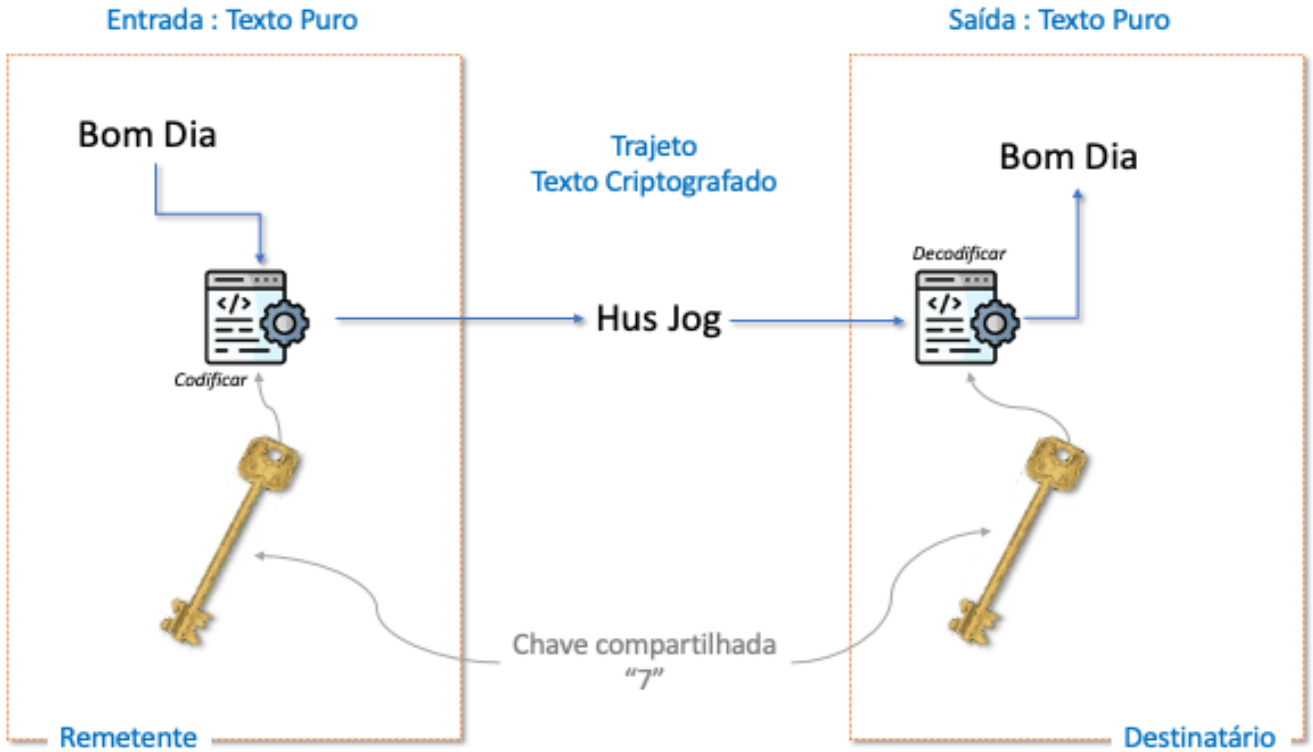
Existem diferentes sistemas de criptografia, que podem ser usado para vários propósitos, como garantir :

- Integridade de dados,
- autenticidade de dados,
- mecanismos de autenticação e não repúdio à informação.

CRIPTOGAFIA, ASSINATURA DIGITAL E CERTIFICADOS

Tipos de Sistemas Criptográficos

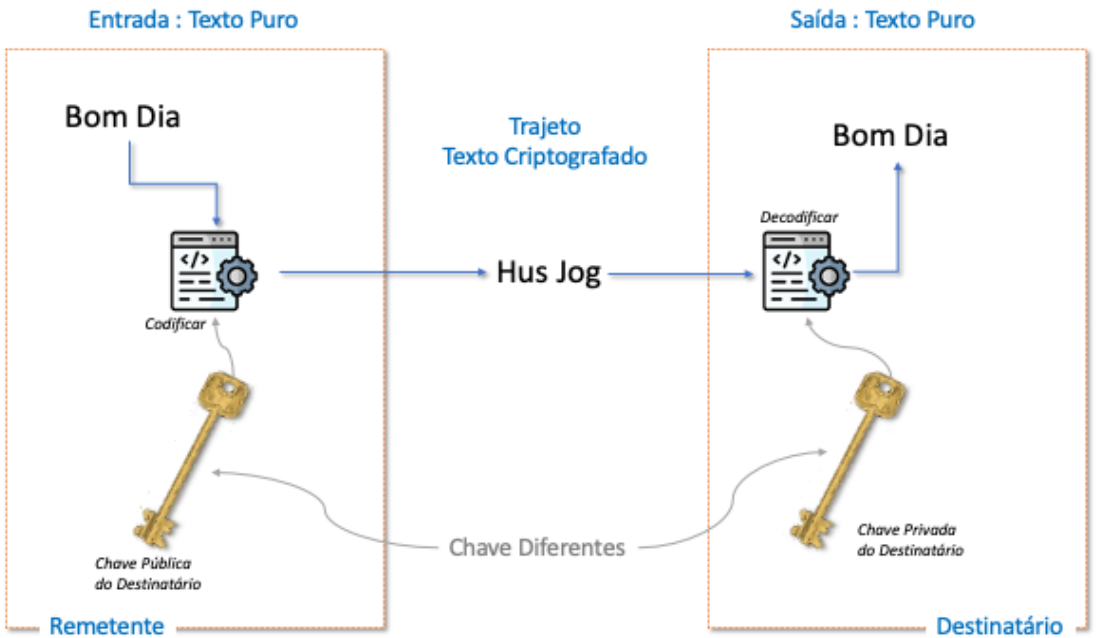
Sistema Simétrico

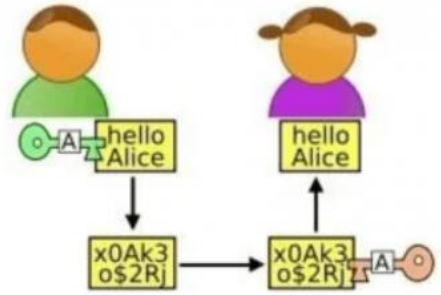


CRIPTOGAFIA, ASSINATURA DIGITAL E CERTIFICADOS

Tipos de Sistemas Criptográficos - Sistema Assimétrico

A criptografia assimétrica é caracterizada pela existência de um par de chaves: a **chave privada** e a **chave pública**.
Uma mensagem encriptada com a chave privada só poderá ser decriptada com a chave pública correspondente, assim como uma mensagem encriptada com uma chave pública só poderá ser decriptada com a chave privada correspondente. Para executar a criptografia assimétrica com intuito de autenticação, a mensagem enviada é criptografada com a chave privada do remetente. Ao receber a mensagem, ela deverá ser decriptografada pelo destinatário utilizando a chave pública do remetente. Se for possível decriptá-la com esta chave pública, é garantida a autenticidade do remetente.
Para garantir a confidencialidade e a integridade do conteúdo de uma mensagem, o remetente deverá criptografar a mensagem com a chave pública do destinatário. Desta forma, apenas o destinatário terá acesso ao conteúdo da mensagem, uma vez que apenas ele possui a chave privada relacionada àquela chave pública.





CRIPTOGAFIA, ASSINATURA DIGITAL E CERTIFICADOS

Assinaturas digitais e certificados

Uma assinatura digital é um método para confirmar se a informação digital foi produzida ou enviada por quem reivindica ser a origem, são criadas utilizando criptografia assimétrica.

É também possível verificar a assinatura digital utilizando um certificado, o que deve ser feito de forma segura, tal como, por exemplo, um token ou smartcard.

SOFTWARE MALICIOSO– MALWARE & CIA

Malware é a combinação das palavras inglesas “malicious” e “software” e se refere a softwares indesejados, tais como vírus, worms , cavalos de Troia e spyware.

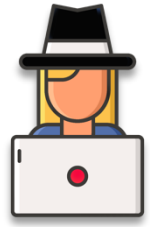
SOFTWARE MALICIOSO– MALWARE & CIA

Conceitos

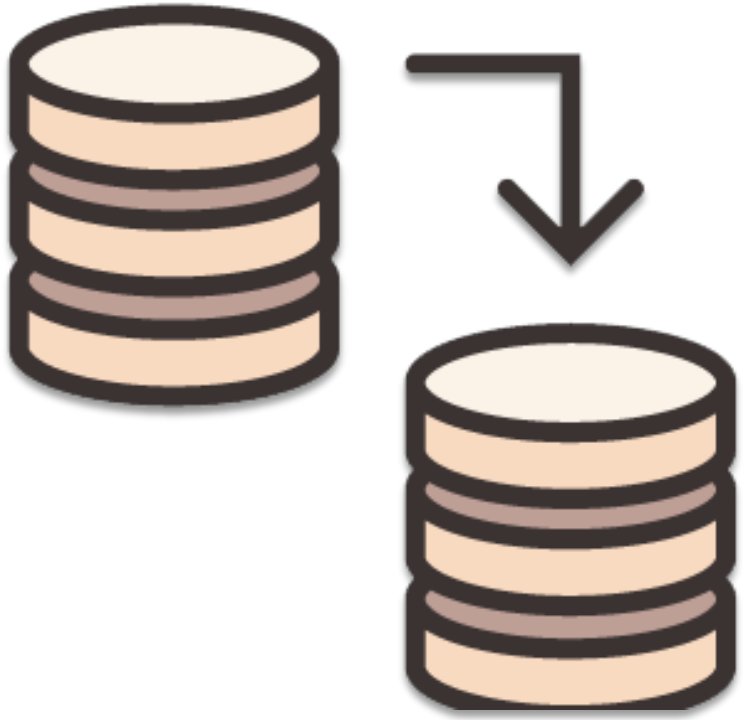
Phishing : Um tipo de fraude na internet que tem como objetivo “pescar” suas informações, principalmente dados de documento e bancários.

Spam : Mensagens indesejadas. O termo é normalmente usado para e-mails indesejados, mas as mensagens publicitárias indesejadas em websites também são consideradas spam.

Hacking : Atividades que têm como objetivo comprometer dispositivos digitais como computadores, smartphones, tablets e até mesmo redes inteiras.



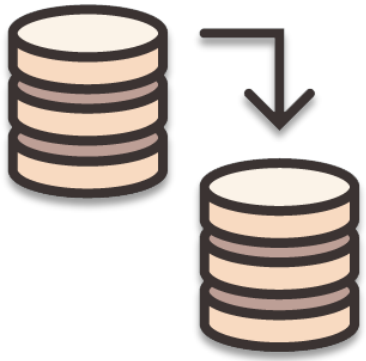
4.5 BACKUP



Backup

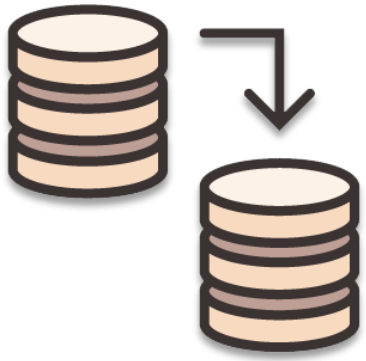
Definição: Backups, ou cópias reservas, visa manter a integridade e a disponibilidade da informação e das instalações computacionais.

As consequências da perda de informação dependem da idade da informação que pode ser recuperada a partir do backup . É importante, portanto:



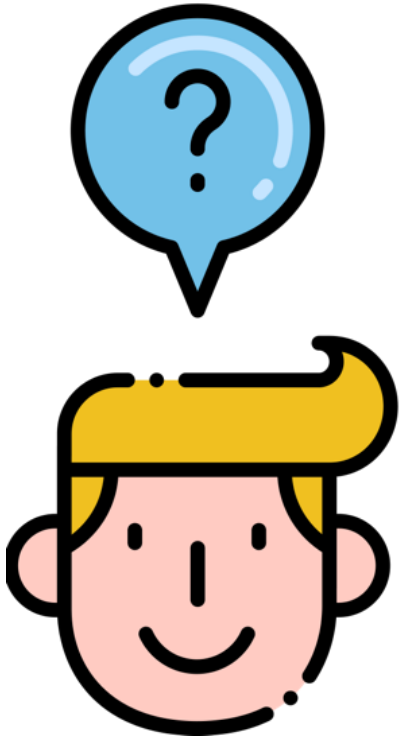
- Considerar o intervalo em que os backups são feitos.
- Quanto tempo podemos nos permitir para recuperar a informação que foi perdida?
- Testar o backup regularmente.
- Manuseá-los de forma segura

Backup



- Em manuseá-los de forma segura devemos considerar :
  - Onde eles são guardados ?
  - Estão próximos ao servidor com os dados originais?
  - Os backups vão para terceiros?
  - Os dados são criptografados?
  - Qual período de armazenamento ?
  - São atendidos os requisitos legais de armazenamento?

4.7 EXERCÍCIOS



EXERCÍCIOS

1. Qual são os 3 tipos de medidas de segurança ? Indique pelo menos um exemplo de cada tipo

Medidas Organizacionais :
- Política de Segurança da Informação
- Acordo de confidencialidade / Códigos de conduta
- Descrição de cargos
- Planos e Programas Conscientização de Segurança
- Auditorias

Medidas Físicas :
Equipe de segurança
Correntes
Cadeados
Login Bio-métrico
No-Breaks
Algo que a pessoa possua

Medidas Técnicas:
Gerenciamento de acesso
Segurança “by Design”
Validações de entradas de dados
Criptografia

5. Legislação e regulamentação

5. Legislação e regulamentação

Tópicos

- Conformidade
- Legislação e regulamentação

LEGISLAÇÃO, REGULAMENTAÇÃO E NORMAS

Legislação e Regulamentos

PNSI

- Decreto 9637/2018: Política Nacional de Segurança da Informação

LGPD

- Lei Geral de Proteção de Dados - Lei 3.709/2018)-

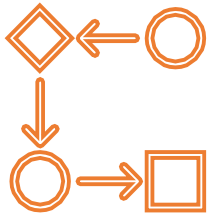
LCC

- Lei de Crimes Cibernéticos (Lei 12.737/2012)

MCI

- Marco Civil da Internet (lei 12.965/2014)

Normas



IEEE

- Institute of Electrical and Electronics Engineers

OWASP - Projeto Aberto de Segurança em Aplicações Web, comunidade online

- Open Web Application Security Project

PCI - Payment Card Industry – Data Security Standard

- Payment Card Industry

LEGISLAÇÃO SOBRE PROTEÇÃO DE DADOS PESSOAIS

Há uma diferença de como UE e EUA tratam em relação à proteção e à privacidade dos dados.

Os EUA utilizam a chamada de abordagem "setorial" à legislação de proteção de dados, contando com uma combinação de legislação, regulamentação e auto-regulamentação, em vez de regulamentos governamentais abrangentes.

6. Referências

- Fundamentos de Segurança da Informação: com base na ISO 27001 e ISO 27002
  Hintzbergen, J., Hintzbergen, K., Smulders, A. e Baars, H., Brasport, 1ª edição, 2018
- Cartilha de Segurança para Internet - https://nic.br/media/docs/publicacoes/13/fasciculo-internet-banking.pdf - acessado em 21/12/2020
- www.iso.org – acessado em 10.10.2020
- https://pt.wikipedia.org/wiki/Computação_em_nuvem - acessado em 21.12.2020
- https://blogbrasil.westcon.com/10-passos-para-garantir-a-seguranca-da-cloud - acessado em 27.12.2020
- https://pt.wikipedia.org/wiki/Big_data - acessado em 27.12.2020
- https://blogbrasil.westcon.com/top-10-melhores-praticas-de-seguranca-em-big-data - acessado em 27.12.2020
- https://cert.br/ - Acessado em 30.12.2020
- https://cartilha.cert.br/malware/ - Acessado em 16.01.2021

PORTAL DO TREINAMENTO!

EDUCAÇÃO EM TI

Agradecemos sua presença em mais este treinamento

PORTAL DO TREINAMENTO!

EDUCAÇÃO EM TI