ANÁLISE DE RISCOS AO SISTEMA DE INFORMAÇÃO	ANÁLISE DE RISCOS AO SISTEMA DE INFORMAÇÃO
O que é uma **Análise de Riscos ao Sistema de Informação**?	**Análise de Riscos:** Uma Análise de Riscos a um sistema informático se resume a uma **análise completa e detalhada de todo um sistema informático buscando averiguar todos os possíveis riscos físicos e lógicos para todo o sistema.** Para isso é preciso coletar o máximo de informações sobre o sistema, ativos físicos e lógicos do sistema e também quanto as possíveis vulnerabilidades que o sistema oferece. A Análise de Riscos é a primeira etapa da implantação de um bom sistema de Segurança da Informação.
Que **componentes** devem estar inclusos a nossa lista de Análise de Riscos?	Na nossa lista devemos nos preocupar em averiguar: **- Processos;** **- Ativos** (Físicos e Lógicos); **- Riscos;** **- Ameaças** (Naturais/Físicas/Intencionais e Não Intencionais)**;** **- Impactos;**
O que envolve a **Análise dos Ativos**?	**Análise dos Ativos:** A Análise dos Ativos é a que vai nos dizer "**OQUE DEVEMOS PROTEGER**", envolve fazer uma análise total de todos os ativos da empresa que envolvam o sistema informático. Estamos falando de ativos tanto **físicos** quanto **lógicos**. Ativos Físicos é tudo o que é material: Computadores, Servidores, Mesas, Cadeiras, Cabos de Alimentação de Rede e etc, já os Ativos Lógicos são os dados: Informações sobre os funcionários, sobre a empresa, softwares utilizados e quaisquer bens imateriais essenciais para a segurança e processos empresariais. Sem uma boa Análise de Ativos, não conheceremos aquilo que devemos proteger, e **se não conhecemos, não conseguimos proteger.**
O que envolve a **Análise dos Processos**?	**Análise dos Processos:** Envolve analisar os processos de trabalho utilizados pela empresa para identificar possíveis vulnerabilidades durante os processos, é a Análise dos Processo que vai nos mostrar "**AONDE DEVEMOS NOS PROTEGER**". Para isso o analista de Sistema de Segurança deve estar a par de todo o processo que envolve o trabalho da empresa, ele deve fazer perguntas como: "É necessário deixar determinada porta aberta?", "Por que não fazer backup ao final desse processo?" e etc.
O que envolve a **Análise dos Riscos**?	**Riscos:** A Análise dos Riscos vai dos dizer "**DO QUE DEVEMOS PROTEGER**", por isso é essencial fazer uma boa Análise de Ativos antes, pois é ela que vai nos mostrar os riscos que nossos ativos estão sujeitos. Essa análise envolve pensar coisas como: "O que poderia acontecer se alguém tivesse acesso aos arquivos do meu servidor?", "O que aconteceria se meu computador pifasse?", "Que danos seriam causados?" Esse tipo de análise iria nos ajudar a **quantificar a probabilidade dum risco se tornar realidade**, **se vale a pena o custo benefício para evitá-lo**, **que impactos acarretaria sobre o meu trabalho**. Isso nos ajudaria a concluir se devemos nos proteger ou não de determinados riscos.
O que envolve a **Análise das Ameças**?	**Análise das Ameaças:** A Análise dos Ameaças é a que vai nos dizer "**DE QUEM DEVEMOS PROTEGER**", ela pode nos mostrar quem são os nossos inimigos. Para isso precisamos ficar atentos a 4 tipos de ameaças: **- Ameaças da Natureza:** Incêndios, Inundações, Tempestades e etc; **- Ameaças Físicas:** Acidentes, Quebra de Equipamentos, Roubos, Ataques de Crackers e etc; **- Ameaças Não Intencionais:** Exposição de Dados não intencional e etc; **- Ameaças Intencionais:** Causadas por vulnerabilidades no sistema, como a ação de Crackers ou traição por parte dos colaboradores;
O que envolve a **Análise dos Impactos**?	**Análise dos Impactos:** A Análise dos Impactos é quem vai nos dizer "**QUE GRAU DE PROTEÇÃO DEVE SER APLICADO**", pois é durante essa análise que vamos averiguar quais serão os impactos duma invasão, roubo de dados, quebra de equipamentos ou acidente. É essa análise que vai nos ajudar a quantificar até que ponto é necessário nos protegermos de uma determinada vulnerabilidade. Nesse ponto devemos nos perguntar: "Que multa teria que pagar se os dados vazassem?", "Que transtorno eu passaria se o computador quebrasse?", "Quanto tempo levaria para me recuperar de um roubo?" e etc.
Quais são **alguns métodos de Análise de Riscos** mais comuns entre os profissionais de Segurança da Informação?	Os profissionais da área de Segurança de informação utilizam de alguns métodos específicos de Análise de Riscos dependendo da situação, esses métodos são: **- Análise Subjetiva;** **- Análise Quantitativa;** **- Análise Qualitativa;** **- Análise Preliminar de Perigos** (APP); **- Análise Preliminar de Riscos** (APR); **- Estudo de Operabilidade de Riscos** (HAZOP); **- Análise de Modos de Falha e Efeitos** (AMFE); **- Análise de Consequências e Vulnerabilidade** (ACV); **- Brainstorming;** **- Diagrama de Causa e Efeito Ishikawa** (Espinha de Peixe); **- Matriz de GUT;**
- reservado para a questão acima -	
Como se dá a **Análise Subjetiva de Riscos**?	**Análise Subjetiva de Riscos:** Essa é uma análise feita somente através de cenários e suposições entre os profissionais de segurança e os profissionais do negócio, que analisam subjetivamente as informações passadas pelos profissionais e supõem cenários ameaçadores que precisam ser minimizados. Esse método é geralmente usado para se chegar a valores aproximados de medidas que devem ser tomadas para visar a segurança, mas ele é o método menos preciso.

ANÁLISE DE RISCOS AO SISTEMA DE INFORMAÇÃO	ANÁLISE DE RISCOS AO SISTEMA DE INFORMAÇÃO
Como se dá a **Análise Quantitativa de Riscos**?	**Análise Quantitativa de Riscos:** Neste tipo de análise, procura-se levantar os valores reais de cada ativo existente nos processos de negócios da organização, em termos do custo de substituição e também ligados à perda de produtividade. Essa análise ajuda a ter uma ideia mais concreta da perca financeira que uma empresa pode ter por não proteger determinados ativos.
Como se dá a **Análise Qualitativa de Riscos**?	**Análise Qualitativa de Riscos:** Nesse tipo de análise, procura-se levantar os valores a serem perdidos diante a exploração de uma determinada vulnerabilidade, e procura-se calcular o valor da perca não apenas tangível, mas também as percas intangíveis, como por exemplo a imagem da empresa, o impacto sobre o emocional dos funcionários, investidores e da liderança. Esse é um método de Análise mais empregado pelas empresas.
Como se dá a **Análise Preliminar de Perigos (APP)**?	**Análise Preliminar de Perigos (APP):** Esse é um tipo de Análise de Riscos nem tanto ligado a segurança da informação em si, mas está mais ligado a segurança física dos colaboradores, do ambitente corporativo e dos ativos físicos. Ela consiste em identificar os possíveis cenários de acidentes e ameaças físicas e classificar esses riscos de acordo com sua frequência e severidade, propondo medidas para a redução dos riscos. Esse tipo de análise é melhor empregado antes da construção das instalações corporativas, mas pode ser usado posteriormente para averiguar a segurança do local.
Como se dá a **Análise Preliminar de Riscos (APR)**?	**Análise Preliminar de Riscos (APR):** Esse é um tipo de Análise de Riscos visa encontrar vulnerabilidades nos processos de trabalho envolvendo os sistemas de informação e quantificar seus impactos sobre o trabalho e a empresa. Nele nós juntamos essas vulnerabilidades as categorizamos com o objetivo de gerar ações preventivas e/ou corretivas.
Como se dá o **Estudo de Operabilidade de Riscos (HAZOP)**?	**Estudo de Operabilidade de Riscos (HAZOP):** O HAZOP ou Hazard and Operabily Study, é um estudo realizado em cima de uma planta de processos com o objetivo de identificar riscos no processo e para produtividade do processo. Esse estudo exige a representação de vários pontos de vista para que haja o máximo de possibilidades possíveis e possam ser criadas medidas que reduzam/eliminem os riscos identificados.
Como se dá a **Análise de Modos de Falha e Efeitos (AMFE)**?	**Análise de Modos de Falha e Efeitos (AMFE):** Nessa técnica de Análise de risco procuramos por possíveis falhas nas vulnerabilidades do sistema por expôr cada um dos componentes vulneráveis a testes de vulnerabilidade reais - claro que tomando precauções para que não haja danos sobre nenhum arquivo. Ao final dos testes coletamos os resultados e detectamos os riscos aos ativos físicos e lógicos e tomamos ações para minimizar ou erradicar esses riscos. Esses testes são muito mais efetivos por expôr o nosso sistema a ameças reais e ver como ele se comporta.
Como se dá a **Análise de Consequências e Vulnerabilidade (ACV)**?	**Análise de Consequências e Vulnerabilidade (ACV):** Essa é uma técnica onde avaliamos as consequências de eventos catastróficos de ampla repercussão, como um ataque Cracker em massa, um desastres natural, queima de vários equipamentos responsáveis por dados de alta relevância, ataque populacional devido a revoltas e outras coisas do tipo.
Como se dá o **Brainstorming**?	**Brainstorming:** Essa não é uma técnica de Análise de Riscos, na verdade é uma técnica que pode ser usada como ferramenta durante uma análise. O Brainstorming consiste em reunir o máximo de pessoas envolvidas numa problemática, mesmo que elas não compreendam muito bem o assunto principal, elas ainda poderão trazer ideias e visões que não são visíveis aos profissionais diretamente envolvidos em resolver o assunto em questão. Essa técnica geralmente é usada quando não conseguimos resolver um assunto e precisamos de olhar o problema de outro ângulo.
Como se dá o **Diagrama de Causa e Efeito de Ishikawa (Espinha de Peixe)**?	**Diagrama de Causa e Efeito de Ishikawa (Espinha de Peixe):** Essa é uma técnica conhecidíssima no meio corporativo, ele foi vulgarizado como "espinha de peixe" por causa do formato do diagrama. Nesse diagrama os envolvidos no problema expõem suas opiniões sobre quais são as **Causas** geradoras do problemas, ou seja, as ameaças. Depois eles tentam expôr quais são ou serão os **Efeitos** gerados a partir dessa ameaça sobre os ativos da empresa. E por fim são propostas soluções para lidar com essas ameaças e seus possíveis efeitos. Essas três etapas são representadas graficamente no diagrama "Espinha de Peixe", o que facilita a visualição e entendimento das Causas, Efeitos e Soluções para um problema.
Como se dá a **Matriz de GUT**?	**Matriz de GUT:** A matriz de GUT é uma técnica usada para entender quais são as ameaças e riscos mais urgentes que deverão ser tratados e montar, por assim dizer, uma "fila de espera" para todos os riscos e ameaças que vão surgindo ao longo do tempo. Por através dessa matriz se torna fácil para o profissional da segurança identificar suas prioridades em tempo hábil para lidar com todas elas.