RESUMO – SEGURANÇA DA INFORMAÇÃO.

1. Ameaça, vulnerabilidade, riscos, insegurança, impacto.
2. Formas de instruções.
3. IDEM um.
4. Criptografia.
5. Ciclo PDCA (melhora contínua/continuada).
6. Gestão da continuidade de negócio
7. NBR, ISO, 27.002 & 27.001.
8. Segurança da informação X negócio corporativo.
9. Sistemas criptografados.

1. Racionalizar um processo de segurança, como é feito por um profissional da área, permite o entendimento e interpretação eficiente e eficaz dos resultados das auditorias, bem como permite uma escolha e seleção mais consistente com necessidade. Como o maior patrimônio das empresas é a informação, como ela cuida, faz toda a diferença no seu negócio, por isso, é importante que toda empresa ao lidar com a informação avalie os riscos, vulnerabilidade e as ameaças que ela pode sofrer.

a. **Ameaça**: É um evento ou atitude indesejável que potencialmente remove, desabilita ou destrói um recurso. As ameaças normalmente aproveitam das falhas de segurança da organização. Possibilidade de um agente (ou fonte de ameaça), explorar acidentalmente ou propositalmente uma vulnerabilidade especifica. (NÃO HÁ CONTROLE).
b. **Vulnerabilidade:** Falha ou fraqueza de procedimento, design, implementação, ou controles internos de um sistema que possa ser acidentalmente ou propositalmente explorada, resultando em uma brecha de segurança ou violação da política de segurança do sistema. Em segurança de computadores, uma vulnerabilidade é uma fraqueza que permite que o atacante reduza a garantia da informação do sistema. Vulnerabilidade é a interseção de três elementos: uma suscetibilidade ou falha do sistema, acesso do atacante a falha e a capacidade do atacante explorar a falha. (PODEM SER TRATADAS).
c. **Riscos:** Qualquer evento que possa causar impacto na capacidade de empresas atingirem seus objetivos de negócio. Probabilidade de uma fonte de ameaça explorar uma vulnerabilidade, resultando em um impacto para organização. (PODEM SER MINIMIZADAS).
d. **Insegurança:** Falta de controle ou medidas de prevenções ataques. Planejamento de contra-ataque a invasões, método de combater o invasor.
e. **Impacto:** Devido a falhas no sistema, o ataque gerar um impacto significativo, causando perda de pacotes, fluxo de produtividade, vasões de informação.

2. Formas de instruções:

3. IDEM um.

4. Criptografia é a prática de codificar e decodificar dados. Quando os dados são criptografados, é aplicado um algoritmo para codificá-los de modo que eles não tenham mais o formato original e, portanto, não possam ser lidos. Os dados só podem ser decodificados ao formato original com o uso de uma chave de decriptografia específica. As técnicas de codificação constituem uma parte importante da segurança dos dados, pois protegem informações confidenciais de ameaças que incluem exploração por malware e acesso não autorizado por terceiros. A criptografia de dados é uma solução de segurança versátil: pode ser aplicada a um dado específico (como uma senha) ou, mais amplamente, a todos os dados de um arquivo, ou ainda a todos os dados contidos na mídia de armazenamento. Em geral, você

geralmente tem contato com a criptografia de dados quando precisa inserir informações de identificação pessoal em um formulário da Web. Sites financeiros, do governo, de escolas e de compras costumam criptografar seus dados para ajudar na proteção contra roubo e fraude. Sempre verifique se os formulários que você preenche na Web são seguros e se os seus dados serão criptografados. Observe se: O URL da página da Web começa com "https": isso indica que seus dados serão criptografados e transferidos por meio de um protocolo seguro. Assim como você espera que os dados confidenciais que insere em um site de terceiros sejam criptografados e protegidos, os dados em seu computador de casa também precisam ser protegidos. Arquivos, senhas, e-mails e backups de dados devem ser criptografados para que estejam a salvo de hackers e ladrões. Existem soluções de segurança versáteis para criptografar e armazenar informações confidenciais.

5. **Ciclo PDCA (melhora contínua/continuada):** uma ferramenta imprescindível ao gerente de projetos. PDCA (planejar ”plan”, fazer “do”, checar “check” e agir “act”.) – responsável por planejar processos, aplica-los, prever falhas, solucioná-las e conferir resultados. O intuito é ajudar a entender, não só como um problema surge, mas também como deve ser solucionado, focando na causa e não nas consequências. Uma vez identificada a oportunidade de melhoria, é hora de colocar em ação atitudes para promover a mudança necessária e, então, atingir os resultados desejados com mais qualidade e eficiência.

6. **Gestão da continuidade de negócio:** é uma abordagem integrada que envolve a mobilização de toda a organização pra gerenciar crises e recuperar as operações após a ocorrência de qualquer evento que cause ruptura operacional. Um plano de recuperação de desastres em TI (PRD) descreve os procedimentos de infraestrutura em casos de desastre. As organizações não tem um plano de contingência que estão sujeitos a impactos significativos e atraso no processo de recuperação. Deve-se então, assegurar a existência de planos adequados para facilitar a recuperação de dados.

7. **NBR, ISO 27,002 & 27,001:** A ISO 27001 é a principal norma que uma organização deve utilizar como base para obter a certificação empresarial em gestão da segurança da informação. Por isso, é conhecida como a única norma internacional auditável que define os requisitos para um Sistema de Gestão de Segurança da Informação (SGSI). **ISO/IEC 27002** é um código de práticas com um conjunto completo de controles que auxiliam aplicação do Sistema de Gestão da Segurança da Informação.

8. **Segurança da informação X negócio corporativo:** A segurança corporativa é um conjunto de medidas de segurança empresarial e de governança corporativa, destinadas a proteger os ativos tangíveis e intangíveis de uma Corporação, contra ameaças decorrentes de ações intencionais ou acidentais, visando garantir a continuidade dos negócios da Organização. Envolve um conjunto de processos, costumes, políticas, procedimentos, normas, regulamentos que regulam a maneira como uma empresa é dirigida, administrativa ou controlada. Balizam o comportamento ético da empresa e de seus colaboradores frente ao mercado de atuação. A segurança corporativa abrange a corporação como um todo os aspectos: humanos, materiais, tecnólogos, informacionais, financeiros, entre outros.

9. **Sistemas criptografados:** qualquer sistema que, dada uma mensagem e uma chave, consiga gerar uma nova mensagem ilegível que possa ser transmitida por canais desprotegidos, sem correr o risco de poder ser compreendida por terceiros sem conhecimento da chave. O sistema só será completo se a mensagem cifrada puder ser recuperada, através de, geralmente, essa mesma ou de outra chave.