MAPA - Material de Avaliação Prática da Aprendizagem

Acadêmico: Mádison Santos Oliveira	**R.A.**23017027-5
Curso: Cibersegurança	
Disciplina: Segurança e Auditória de Sistemas	

Instruções para Realização da Atividade

1. Todos os campos acima deverão ser devidamente preenchidos.
2. É obrigatória a utilização deste formulário para a realização do MAPA.
3. Esta é uma atividade individual. Caso identificado cópia de colegas, o trabalho de ambos sofrerá decréscimo de nota.
4. Utilizando este formulário, realize sua atividade, salve em seu computador, renomeie e envie em forma de anexo. Antes de selecionar a opção de 'Finalizar' a atividade no sistema, verifique o arquivo anexado, pois arquivos em branco ou incorretos **não** poderão ser substituídos após a finalização.
5. Formatação exigida para esta atividade: documento Word, Fonte Arial ou Times New Roman tamanho 12, Espaçamento entre linhas 1,5, texto justificado.
6. Ao utilizar quaisquer materiais de pesquisa referencie conforme as normas da ABNT.
7. Critérios de avaliação: Utilização do template (Formulário Padrão); Atendimento ao Tema; Constituição dos argumentos e organização das Ideias; Correção Gramatical e atendimento às normas ABNT.
8. Procure argumentar de forma clara e objetiva, de acordo com o conteúdo da disciplina.

Em caso de dúvidas, entre em contato com seu Professor Mediador.
Bons estudos!

AGORA É COM VOCÊ!

Para realizar o controle de vulnerabilidades técnicas e mitigar os riscos potenciais associados a essas vulnerabilidades em uma empresa, é essencial seguir rigorosamente as normas estabelecidas pela ABNT NBR ISO/IEC 17799:2005. Esta norma aborda técnicas de segurança e fornece um código de prática para a gestão da segurança da informação. A implementação de políticas de segurança, normas internas e monitoramento e análise de segurança são passos cruciais para reduzir as possíveis brechas que poderiam permitir acesso não autorizado a informações confidenciais da empresa. A seguir, destaco procedimentos robustos que garantirão confiabilidade e segurança: Capacitar os colaboradores é fundamental para fortalecer a segurança da empresa. Ao treiná-los sobre os procedimentos de segurança, como rotinas e processos de análise de e-mails recebidos, ataques de engenharia social e phishing, pode-se reduzir significativamente a possibilidade de um ataque bem-sucedido. Essa capacitação não apenas fortalece a segurança, mas também cria uma cultura de conscientização, onde os colaboradores são capazes de identificar e responder adequadamente a possíveis ameaças, contribuindo assim para a proteção dos ativos da empresa.

A identificação de vulnerabilidades é essencial para fortalecer a segurança da empresa. Através desse processo, se examina minuciosamente programas, sistemas e hardwares em busca de possíveis falhas existentes. Os softwares serão meticulosamente testados para identificar possíveis vulnerabilidades, como má configuração ou falta de implementação de medidas de segurança adequadas. Além disso, softwares desenvolvidos sem a devida atenção à segurança podem conter arquivos maliciosos, com o intuito de proporcionar acesso não autorizado. Ao realizar essa análise detalhada, identifica-se e corrigi-se as vulnerabilidades antes que sejam exploradas por indivíduos mal-intencionados.

Priorização de Vulnerabilidades: Uma vez identificadas as vulnerabilidades, é importante priorizá-las com base em sua gravidade e potencial impacto no negócio.

Vulnerabilidades críticas e de alto impacto devem ser tratadas com urgência, enquanto as de menor impacto podem ser abordadas posteriormente.

Implementação de Medidas de Controle: Após priorizar as vulnerabilidades, é hora de implementar medidas de controle para mitigar ou eliminar os riscos associados a essas vulnerabilidades. Isso pode envolver a aplicação de patches de segurança, configurações de segurança adequadas, implementação de firewalls, uso de criptografia, entre outras medidas de segurança.

Teste de Controles Implementados: Antes de colocar os controles em produção, é importante testá-los para garantir que funcionem conforme o esperado e não causem impactos indesejados nos sistemas ou aplicativos da empresa. Isso pode incluir testes de penetração, testes de intrusão e outros métodos de teste de segurança.

Monitoramento Contínuo: Uma vez que os controles tenham sido implementados, é crucial monitorá-los continuamente para detectar e responder a novas vulnerabilidades ou tentativas de exploração. Isso pode envolver o uso de sistemas de detecção de intrusão, monitoramento de logs, entre outras técnicas de monitoramento de segurança.

Atualização Regular: Por fim, é importante manter os controles de segurança atualizados e revisar periodicamente a postura de segurança da empresa para garantir que ela permaneça resiliente contra as ameaças em evolução.

Uma potencial vulnerabilidade que poderia ser explorada dentro de uma empresa é a falta de atualizações de segurança em software e sistemas. Se os sistemas não forem regularmente atualizados com os patches mais recentes de segurança, podem ser explorados por invasores que se aproveitam de vulnerabilidades conhecidas para comprometer os sistemas e acessar informações sensíveis da empresa. Portanto, garantir que os sistemas sejam regularmente atualizados com os últimos patches de segurança é uma medida crucial para reduzir esse tipo de vulnerabilidade.

É fundamental estabelecer procedimentos claros para o gerenciamento de patches e atualizações, garantindo que sejam aplicados de maneira oportuna e eficiente. Isso pode incluir a implementação de políticas que exijam a instalação automática de patches críticos, a realização de testes de compatibilidade antes da implementação

de atualizações em larga escala e o monitoramento constante de fontes confiáveis de informações sobre vulnerabilidades e correções disponíveis. Além disso, é importante manter um inventário atualizado de todos os sistemas e software utilizados pela empresa, facilitando o acompanhamento e a aplicação de atualizações necessárias. Ao priorizar a segurança cibernética e a manutenção proativa dos sistemas, as empresas podem reduzir significativamente sua exposição a ameaças e ataques cibernéticos.