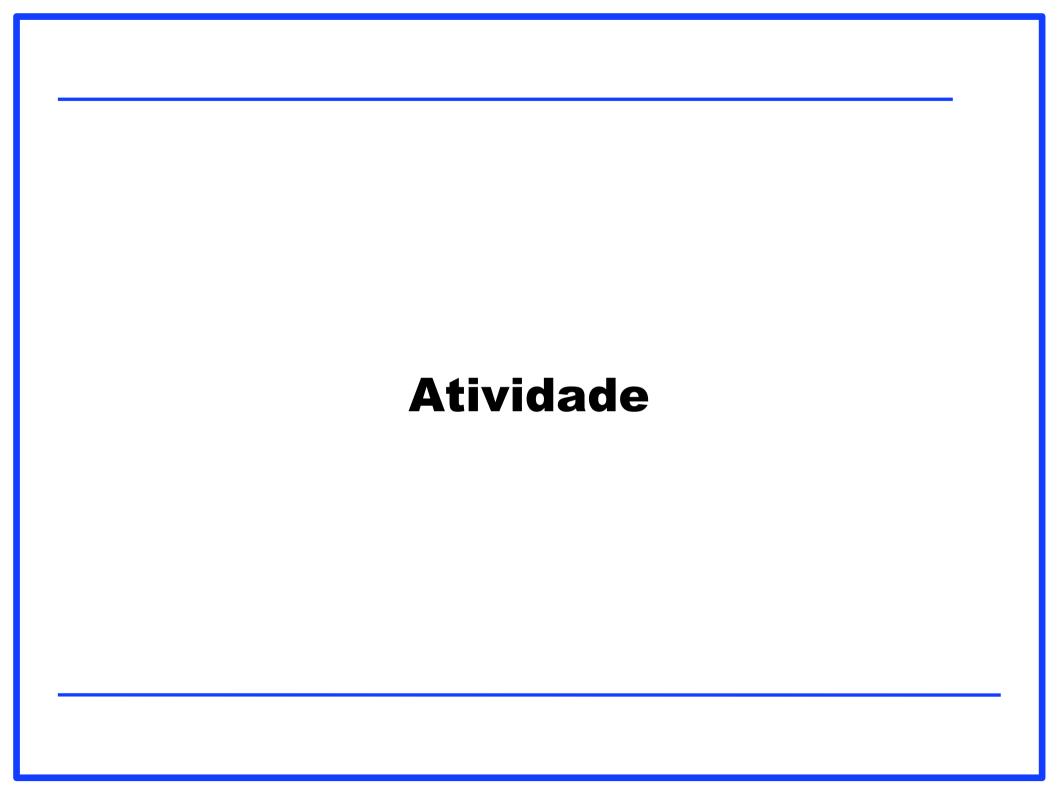


Introdução à Segurança da Informação

Prof. Dr. José Augusto de Sena Quaresma Jq.quaresma12@gmail.com



Em equipes (7 pessoas)

- Levando em consideração as notícias relacionadas no trabalho anterior (Pesquisa sobre incidentes)
- Escolher e classificar quais vulnerabilidades foram utilizadas para gerar o incidente. Justificar.
- Identificar o tipo de incidente que a notícia seria classificada
- Indicar o risco que não foi mitigado
- Identificar os tópicos da norma que estão associados aos incidentes
- Entrega do trabalho é única
- Quantidade de notícias é pelo menos 4
- Prazo fase 02 Próxima semana

Mecanismos de controle

Elementos da segurança

- > Físico
- Lógicos
- Administrativos

Elementos da segurança – Físico

- Medidas físicas para proteger os elementos da segurança da informação de uma empresa
- Barreiras, proteções e contingencia
- Controle de acesso físico
- Armazenamento seguro de mídias físicas
- Ambiente controlado
- Backup de energia
- Backup de dados
- Proteção de desastres

Elementos da segurança – Lógicos

- Referem-se aos aspectos não físicos, como políticas, procedimentos, software e configurações que são implementados para proteger os ativos de informação de uma organização.
- Eles desempenham um papel crucial na prevenção, detecção e resposta a ameaças cibernéticas.

Elementos da segurança – Lógicos

- Controles de Acesso: Mecanismos que garantem que apenas usuários autorizados tenham acesso a recursos de informação específicos. Isso pode incluir autenticação de usuários por meio de senhas, autenticação multifatorial, tokens de segurança e controle de acesso baseado em funções.
- Criptografia: Técnica que transforma dados em uma forma ilegível para proteger a confidencialidade das informações. A criptografia é usada para proteger a comunicação de rede, armazenamento de dados sensíveis e autenticação.

Elementos da segurança – Lógicos

- Controle de Integridade: Mecanismos que garantem que os dados não sejam alterados de forma não autorizada. Isso pode envolver a implementação de assinaturas digitais, controle de versões e checksums.
- Controle de Autenticidade: Verificação da identidade das partes envolvidas em uma transação ou comunicação. Isso é alcançado por meio de técnicas como autenticação de usuários, certificados digitais e assinaturas digitais.

- Referem-se às políticas, procedimentos, treinamento e governança que são estabelecidos e mantidos pela administração da organização para garantir a proteção adequada dos ativos de informação.
- Esses elementos desempenham um papel fundamental na definição de uma cultura de segurança da informação dentro da organização e na garantia de conformidade com requisitos regulatórios.

Políticas de Segurança da Informação:

Documentos formais que estabelecem diretrizes e regras para proteger os ativos de informação da organização. As políticas abordam questões como acesso a dados, gerenciamento de senhas, uso aceitável de recursos de TI, entre outros.

➤ Treinamento e Conscientização em Segurança da Informação: Programas de treinamento e conscientização projetados para educar os funcionários sobre práticas seguras de segurança da informação e reconhecimento de ameaças. Isso inclui treinamento sobre políticas de segurança, phishing, engenharia social e melhores práticas de segurança.

Gestão de Incidentes de Segurança: Procedimentos para lidar com incidentes de segurança da informação de forma eficaz e eficiente. Isso inclui a implementação de planos de resposta a

incidentes, comunicação de incidentes, investigação forense e ação corretiva.

Governança de Segurança da Informação: Estrutura de governança estabelecida para supervisionar e direcionar as atividades de segurança da informação dentro da organização. Isso inclui a definição de papéis e responsabilidades, a criação de comitês de segurança e a garantia de conformidade com regulamentos e padrões.

Conformidade Regulatória: Garantir que as práticas de segurança da informação estejam em conformidade com requisitos regulatórios, leis de privacidade e padrões da indústria. Isso inclui a realização de auditorias de conformidade, relatórios regulatórios e manutenção de registros de conformidade.

Revisão e Melhoria Contínua: Processos para revisar regularmente as políticas, procedimentos e controles de segurança da informação, identificar áreas de melhoria e implementar medidas corretivas para fortalecer a postura de segurança da organização.

Auditoria: Sistemas de Logs

Sistemas de Logs

- Um registro de alterações e eventos em sistemas de TI.
- Diversas aplicações, serviços, sistemas operacionais e dispositivos de rede geram logs de eventos

Formato do Log

- A hora em que o evento ocorreu
- Detalhes do que aconteceu e quando
- Informação sobre qual usuário causou o evento
- Detalhes sobre a reação do sistema, incluindo mensagens como "Falha de auditoria", "Requisição aceita" ou "Acesso negado".

Passos do log de auditoria

- Coleta de logs
- Agregação de Logs
- Normalização de logs
- Correlação de eventos
- Análise de logs

Coleta de logs

- Quais computadores, software, dispositivos e outros sistemas para coletar os eventos
- Quais configurações usar para cada log, como se o tamanho padrão de log será utilizado
- Como os dados serão armazenados e coletados
- Como os padrões de tempo normais devem parecer (origem e fuso horário)
- Obs .: Coletar tudo é possível porém é necessário pensar em espaço e custos relacionados

Agregação de Logs

- Onde os dados de logs vão ser armazenados
- Implementação de um sistema gerenciamento de logs
- Repositório dos logs deve estar fora de alcance para alteração. Deve ser apenas de consulta.

Normalização dos logs

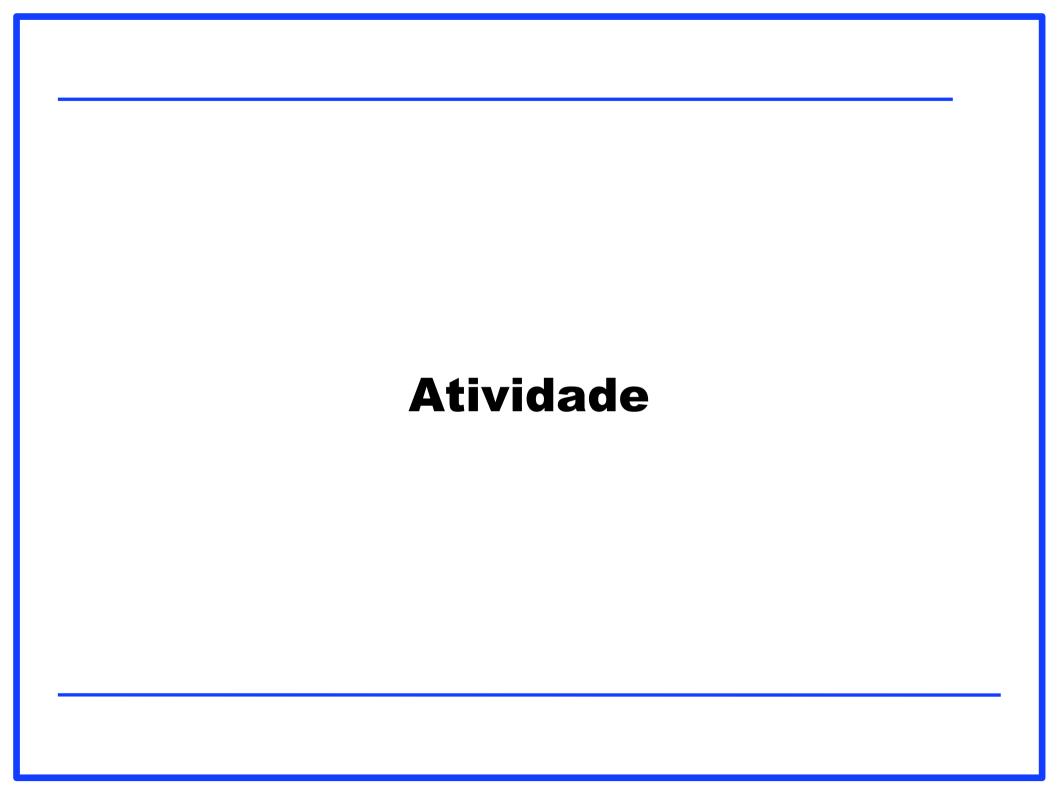
- O ideal é que todas as aplicações/ sistemas já enviem os dados em um determinado padrão para manter a consistência e seja fácil de consulta o log.
- Porém as aplicações podem mandar em diversos formatos e nessa situação pode ser realizada uma normalização dos logs para exibição de consulta

Correlação dos eventos

Encontrar relações entre os eventos em diferentes logs de sistemas ou aplicações no servidor.

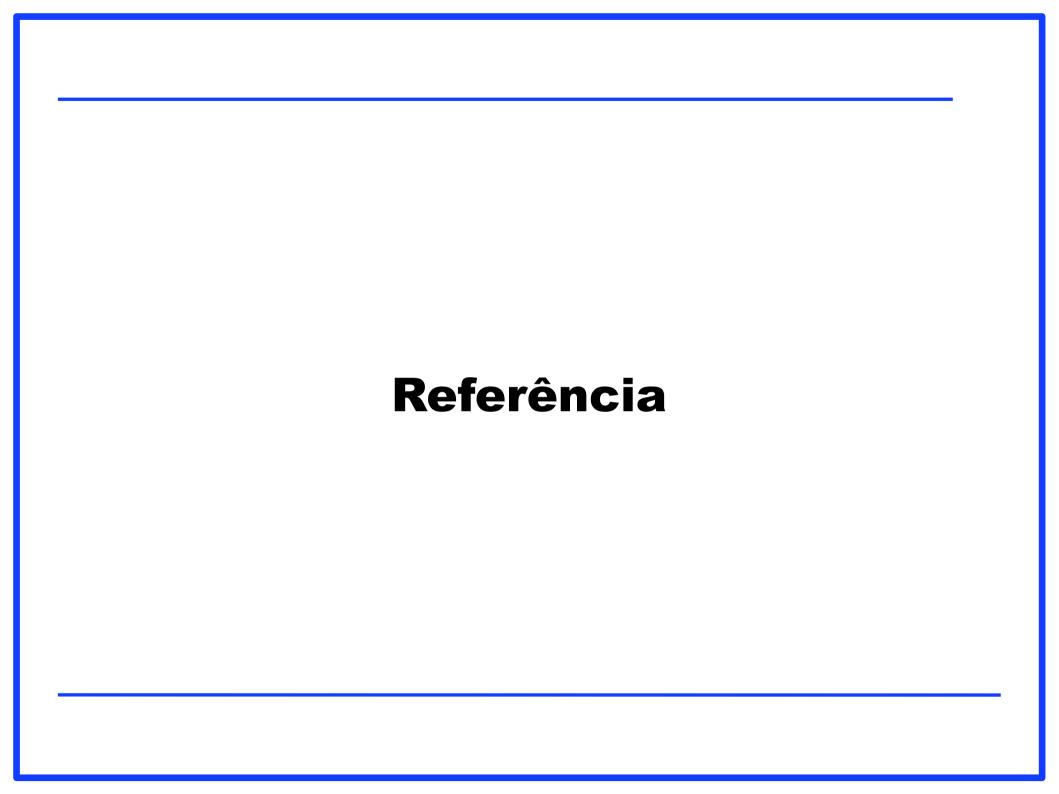
Análise de logs

- O processo de análise de logs identifica se uma ameaça passou pelo sistema ou se temos ações anormais
- Geralmente precisa-se de inteligência de dados para encontrar e apresentar padrões que devem ser verificados.
- A análise permite o rastreamento do erro do cliente por diversos sistemas da empresa ou identificar o sistema que apresentou o erro.



Projeto – Equipe

Fase 03 – Descrever dois elementos administrativos da segurança que podem ser pensados após a ocorrência dos incidentes dentro das organizações



Referencias

- CABRAL, Carlos.; CAPRINO, Willian. Trilhas em Segurança da Informação: caminhos e ideias para a proteção de dados.
 Rio de Janeiro: Brasport, 2015. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160689
- HINTZBERGEN, Jule. et. al. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002.. 1. Rio de Janeiro: Brasport, 2018. Disponível em: https://plataforma.bvirtual.com.br/Acervo/Publicacao/160044
- https://aiqon.com.br/blog/principios-de-monitoramento-deeventos-e-de-logs-de-auditoria/
- Notas de aula do professor Dr. Daniel Caetano.