# Práticas recomendadas para uma documentação eficaz

**Documentação** é qualquer forma de conteúdo registrado que é usado para uma finalidade específica e é essencial no Campo da Segurança. As Equipes de segurança usam a documentação para apoiar investigações, concluir tarefas e comunicar descobertas. Esta leitura explora os Benefícios da documentação e fornece uma lista de práticas comuns para ajudá-lo a criar uma documentação eficaz em sua carreira na área de segurança.

## Benefícios da documentação

Você já aprendeu sobre muitos tipos de documentação de segurança, incluindo manuais, relatórios finais e muito mais. ASe você também aprendeu, a documentação eficaz tem três Benefícios:

1. Transparência
2. Padronização
3. Clareza

### ****Transparência****

Na segurança, a transparência é fundamental para demonstrar a conformidade com os regulamentos e os processos internos, atender aos Requisitos de seguro e para os processos legais. **A cadeia de custódia** é o processamento da documentação da posse e do controle de evidências durante o ciclo de vida de um incidente. A cadeia de custódia é um exemplo de como a documentação produz transparência e uma trilha de auditoria.

### ****Padronização****

A padronização por meio de processos e procedimentos que podem ser repetidos apoia os esforços de Melhoria contínua, ajuda na transferência de conhecimento e facilita a integração de novos Membros da equipe. **Os padrões** são referências que informam como definir políticas.

Você aprendeu como o NIST fornece vários frameworks de segurança que são usados para melhorar as medidas de segurança. Da mesma forma, as organizações estabelecem seus próprios padrões para atender às suas necessidades comerciais. Um exemplo de documentação que estabelece padronização é um **plano de resposta a incidentes**, que é um documento que descreve os procedimentos a serem adotados em cada etapa da resposta a incidentes. Os planos de resposta a incidentes padronizam o processamento de resposta de uma organização ao delinear os procedimentos antes de um incidente. Ao documentar o plano de resposta a incidentes de uma organização, você cria um padrão que as pessoas seguem, mantendo a consistência com processos e procedimentos que podem ser repetidos.

### ****Clareza****

O ideal é que toda documentação ofereça clareza ao seu público. A documentação clara ajuda as pessoas a acessar rapidamente as informações de que precisam para que possam tomar as medidas necessárias. Os analistas de segurança devem documentar o raciocínio por trás de qualquer ação que tomem, para que fique claro para a equipe por que um alerta foi encaminhado ou fechado.

## Práticas recomendadas

Como profissional de segurança, você precisará aplicar as práticas recomendadas de documentação em sua carreira. Aqui estão algumas diretrizes gerais que devem ser lembradas:

### ****Conheça seu público****

Antes de começar a criar a documentação, considere seu público e as necessidades dele. Por exemplo, um resumo de incidente escrito para um gerente do Centro de operações de segurança (SOC) será redigido de forma diferente de um resumo redigido para um CEO (Chief Executive Officer). O gerente do SOC pode entender a linguagem técnica de segurança, mas um CEO talvez não. Adapte seu documento para atender às necessidades de seu público.

### ****Seja conciso****

Talvez você tenha a tarefa de criar uma documentação longa, como um relatório. Mas quando a documentação é muito longa, as pessoas podem se sentir desencorajadas a usá-la. Para garantir que sua documentação seja útil, estabeleça a finalidade imediatamente. Isso ajuda as pessoas a identificar rapidamente o objetivo do documento. Por exemplo, os resumos executivos descrevem os principais fatos de um incidente no início de um relatório final. Esse resumo deve ser breve, de modo que possa ser facilmente folheado para identificar as principais descobertas.

### ****Atualize regularmente****

Na segurança, novas vulnerabilidades são descobertas e exploitadas constantemente. A documentação deve ser revisada e atualizada regularmente para acompanhar o cenário de ameaças em evolução. Por exemplo, depois que um incidente é resolvido, uma revisão abrangente do incidente pode identificar lacunas nos processos e procedimentos que exigem mudanças e atualizações. Ao atualizar regularmente a documentação, as equipes de segurança ficam bem informadas e os planos de resposta a incidentes permanecem atualizados.

## Principais conclusões

A documentação eficaz produz Benefícios para todos em uma organização. Saber como criar documentação é uma habilidade essencial para um analista de segurança. ASe continuar em sua jornada para se tornar um profissional de segurança, não deixe de considerar essas práticas para criar uma documentação eficaz.