INDICADORES DE SEGURANÇA DA INFORMAÇÃO

- Taxa de Incidentes de Segurança: Isso inclui o número de incidentes de segurança reportados, como violações de dados, malware, ataques de phishing, etc. Uma alta taxa pode indicar a necessidade de melhorias nas medidas de segurança.

- Tempo Médio de Detecção (MTTD): Refere-se ao tempo médio que leva para detectar uma violação ou incidente de segurança após a ocorrência. Um MTTD curto é desejável, pois significa detecção rápida.

- Tempo Médio de Resposta (MTTR): Indica o tempo médio necessário para responder e remediar um incidente de segurança após sua detecção. Um MTTR curto é importante para minimizar o impacto de um incidente.

- Taxa de Falsos Positivos: Mede a proporção de alertas de segurança que são falsos positivos, ou seja, alertas que não representam uma ameaça real. Reduzir a taxa de falsos positivos ajuda a concentrar os recursos onde são realmente necessários.

- Taxa de Conformidade: Avalia o grau em que a organização está em conformidade com regulamentações de segurança, políticas internas e melhores práticas. A não conformidade pode resultar em riscos significativos.

- Número de Vulnerabilidades Não Corrigidas: A contagem de vulnerabilidades conhecidas que ainda não foram corrigidas. Uma alta contagem pode representar um risco de segurança significativo.

- Taxa de Atualização de Software: Mede a rapidez com que os sistemas e aplicativos são atualizados com patches de segurança. Manter sistemas atualizados é crucial para evitar explorações de vulnerabilidades conhecidas.
- Nível de Conscientização dos Colaboradores: Avalia o nível de conscientização dos colaboradores sobre práticas de segurança, com

base em testes de conscientização ou avaliações regulares.

- Número de Acessos Não Autorizados: Monitora a quantidade de tentativas ou incidentes de acesso não autorizado aos sistemas ou dados da organização.

- Uso Anômalo de Credenciais: Rastreia atividades suspeitas que possam indicar o uso não autorizado de credenciais de usuário, como logins fora do horário comercial ou de locais não usuais.

- Taxa de Sucesso de Testes de Intrusão: Mede quantos testes de intrusão bem-sucedidos ocorreram em relação ao total de testes realizados. Uma taxa alta de sucesso indica falhas de segurança.

- Disponibilidade de Sistemas: A percentagem de tempo em que os sistemas críticos estão disponíveis e operacionais. A indisponibilidade prolongada pode ser prejudicial para a organização.

- Taxa de Relatórios de Incidentes: A proporção de incidentes de segurança relatados em comparação com os incidentes não relatados. Uma alta taxa de relatórios é positiva, pois os incidentes podem ser tratados adequadamente.

- Tempo Médio entre Ataques (Mean Time Between Attacks - MTBA): Mede o tempo médio entre diferentes ataques bem-sucedidos. Um MTBA mais longo indica uma melhor resistência contra ataques frequentes.

- Taxa de Infecção por Malware: Mede a frequência com que sistemas são infectados por malware. Uma baixa taxa é desejável.