KIRALY
TECNOLOGIA
TECNOLOGIA DA INFORMAÇÃO. A LINGUAGEM DO FUTURO.

Analista de Segurança da Informação

Um analista de segurança da informação é um profissional especializado em proteger os ativos digitais de uma organização contra ameaças cibernéticas. Suas responsabilidades incluem identificar vulnerabilidades em sistemas e redes, desenvolver e implementar medidas de segurança, monitorar atividades suspeitas, responder a incidentes de segurança, realizar análises forenses e educar os funcionários sobre práticas seguras de TI. Eles desempenham um papel crucial na proteção dos dados confidenciais e na garantia da conformidade com regulamentos de segurança, contribuindo para a confiança e integridade dos sistemas de informação da organização.

Análise de Vulnerabilidades: O analista conduz uma avaliação completa dos sistemas de TI da empresa, identificando possíveis vulnerabilidades em sua infraestrutura, como falhas de configuração, software desatualizado ou lacunas na segurança da rede

KIRALY TECNOLOGIA
TECNOLOGIA DA INFORMAÇÃO. A LINGUAGEM DO FUTURO.

Implementação de Medidas de Segurança: Com base na análise, o analista implementa medidas proativas de segurança, como a configuração de firewalls, sistemas de detecção de intrusos e proteção contra malware. Eles também garantem que todos os sistemas e aplicativos estejam atualizados com os patches de segurança mais recentes.

Monitoramento em Tempo Real: O analista configura sistemas de monitoramento para acompanhar continuamente a atividade da rede e identificar comportamentos suspeitos. Eles utilizam ferramentas de análise de logs e inteligência de ameaças para detectar possíveis ataques ou violações de segurança.

KIRALY TECNOLOGIA
TECNOLOGIA DA INFORMAÇÃO. A LINGUAGEM DO FUTURO.

Resposta a Incidentes: Se ocorrer um incidente de segurança, como uma tentativa de invasão ou um ataque de phishing direcionado aos clientes, o analista lidera a resposta imediata. Isso pode incluir a isolamento de sistemas comprometidos, a análise forense para determinar a extensão do comprometimento e a notificação às autoridades e partes interessadas relevantes.

***Treinamento e Conscientização*:** Além disso, o analista fornece treinamento regular aos funcionários sobre práticas de segurança cibernética, como reconhecer e relatar phishing, criar senhas seguras e proteger informações confidenciais. Isso ajuda a fortalecer a cultura de segurança da empresa e reduzir o risco de violações de dados.