



Processo Seletivo 01876/2024

Conheça aqui a descrição das atividades relacionadas ao cargo Supervisor de Segurança da Informação

Principais Responsabilidades:

1. Supervisionar o desenvolvimento e implementação de políticas e procedimentos de segurança da informação do Sistema FIESC, definindo papéis, responsabilidades e ações a serem realizadas, a fim de proteger os ativos de informação contra ameaças e riscos.
2. Monitorar e avaliar a eficácia dos controles de segurança, acompanhando constantemente a aplicação dos controles de segurança, analisando indicadores de desempenho e realizando testes periódicos, para garantir que os objetivos de segurança estejam sendo alcançados.
3. Supervisionar incidentes de segurança da informação, propondo planos de resposta a incidentes, investigando e documentando ocorrências, implementando ações corretivas e de melhoria, visando minimizar os impactos e evitar a recorrência de incidentes.
4. Realizar análises de riscos e vulnerabilidades, por meio da identificação, análise e tratamento dos riscos associados aos ativos de informação, priorizando as ações com base na criticidade e probabilidade de ocorrência, a fim de garantir a continuidade dos processos de negócio.
5. Supervisionar a implementação de controles de segurança, monitorando a instalação, configuração e manutenção de ferramentas de segurança, como firewalls, sistemas de detecção e prevenção de intrusão, antivírus, entre outros, para proteger a infraestrutura tecnológica.
6. Fornecer treinamento e conscientização em segurança da informação, por meio do desenvolvimento e execução de programas de capacitação e sensibilização para os colaboradores, abordando temas como ameaças, melhores práticas e responsabilidades, com o objetivo de promover uma cultura de segurança.
7. Supervisionar o acesso aos sistemas e informações, estabelecendo e mantendo processos de concessão, revisão e revogação de acessos, de acordo com os princípios de menor privilégio e necessidade de conhecimento, para evitar usos indevidos e acesso não autorizado.
8. Supervisionar a implementação de backups e planos de recuperação de desastres, por meio do acompanhamento da execução de backups regulares e a elaboração de planos de continuidade de negócios, a fim de garantir a disponibilidade das informações críticas e a recuperação em caso de incidentes.
9. Estabelecer e manter controles de criptografia, por meio da proposição e implementação de políticas de criptografia para a proteção de informações confidenciais e sensíveis durante o armazenamento e transmissão, de acordo com os requisitos legais e regulatórios.
10. Monitorar e responder a ameaças cibernéticas, acompanhando os alertas de segurança, analisando as ameaças em tempo real e aplicando medidas de mitigação, visando identificar, prevenir e responder efetivamente a ataques cibernéticos.
11. Supervisionar os fornecedores e serviços terceirizados, avaliando os riscos relacionados a terceiros, estabelecer e monitorar os contratos de prestação de serviços, a fim de garantir que os níveis de segurança da informação sejam mantidos.
12. Elaborar relatórios e métricas de segurança, por meio da coleta, análise e report de indicadores de desempenho, estatísticas e informações sobre a situação da segurança da informação, para embasar a tomada de decisão e a melhoria contínua do programa de segurança.
13. Atender a requisitos legais e regulatórios, por meio da identificação, interpretação e garantia do cumprimento das leis, normas e regulamentos aplicáveis à segurança da informação, evitando sanções e mantendo a conformidade.
14. Participar de comitês e grupos de trabalho de segurança, representando a área de segurança da informação em reuniões, comitês e grupos de trabalho, contribuindo com a discussão e alinhamento de estratégias e ações de segurança.
15. Manter-se atualizado sobre ameaças e soluções de segurança, por meio do acompanhamento constantemente das tendências, melhores práticas e inovações em segurança da informação, participando de treinamentos, lendo publicações e interagindo com a comunidade de segurança, a fim de aprimorar continuamente as práticas de segurança adotadas.
16. Supervisionar a elaboração e atualização de justificativas, pareceres e termos de referência para atender as necessidades técnicas nos processos de desenvolvimento e melhoria das estruturas de TI alinhadas às necessidades de negócio do Sistema FIESC.
17. Executar outras atividades correlatas a critério do superior imediato.