**SUGESTÕES DE QUESTIONAMENTOS PARA OPERADORES/FORNECEDORES DE SOFTWARE**

|  |  |
| --- | --- |
| Nome do órgão, entidade ou nome da divisão | |
| Número: | Número sequencial da Entrevista |
| Data: | DD/MM/AAAA |
| Hora: | <HH:MM> |
| Local: | <se presencial, inserir endereço. Se online, indicar aplicativo utilizado e link> |

|  |  |  |
| --- | --- | --- |
| Entrevistados | Setor | Status |
| <Inserir o nome do agente público> | <Inserir setor ao qual faz parte o agente público> | <presente, ausente ou ausência justificada> |

1. A organização possui um controle da implementação e documentação do sistema?
2. A organização possui definidas as funções e responsabilidades associadas à gestão de vulnerabilidades técnicas, incluindo o monitoramento de vulnerabilidades, a avaliação de risco de vulnerabilidades, correções e acompanhamento dos ativos ou demais responsabilidades jurídicas e de segurança da informação?
3. Há um gerenciamento de configurações para hardware e software do serviço que é oferecido pelo operador, de modo a evitar o comprometimento da disponibilidade do serviço?
4. O operador possui ambientes de desenvolvimento, homologação e produção segregados, de modo a reduzir riscos de acessos ou modificações não autorizadas no ambiente de produção?
5. O operador possui controles que garantam a confidencialidade e integridade dos dados em trânsito sobre redes, de modo a proteger os sistemas e aplicações a elas conectadas?
6. A organização possui mecanismos de registro (log) e monitoramento de ameaças para habilitar a gravação e detecção de ações que possam afetar, ou ser relevante para a segurança da informação?
7. Os requisitos relacionados com segurança da informação são incluídos nos requisitos para novos sistemas de informação ou melhorias dos sistemas de informação existentes?
8. As informações envolvidas nos serviços de aplicação que transitam em redes públicas são protegidas de atividades fraudulentas, disputas contratuais, divulgação e modificações não autorizadas?
9. A organização possui uma avaliação de riscos detalhada e uma seleção de controles apropriados para serviços de aplicação em redes públicas?
10. Aplicações críticas de negócios são analisadas criticamente e testadas quando plataformas operacionais são mudadas, para garantir que não haverá nenhum impacto adverso na operação da organização ou na segurança?
11. Modificações em pacotes de software são desencorajadas e estão limitadas às mudanças necessárias, e essas mudanças são estritamente controladas?
12. A organização estabelece princípios para projetar sistemas seguros, documentados, e estes mantidos e aplicados para qualquer implementação de sistemas de informação?
13. A organização estabelece e protege adequadamente os ambientes seguros de desenvolvimento, como esforços de integração e desenvolvimento de sistemas, que cubram todo o ciclo de vida de desenvolvimento de sistemas?
14. A organização supervisiona e monitora se as atividades de desenvolvimento de sistemas terceirizados contemplam a segurança da informação em todas as suas fases?
15. Testes de funcionalidade de segurança são realizados durante o desenvolvimento de sistemas?
16. A organização possui diretrizes sobre responsabilidades e procedimentos em relação à gestão de incidentes de segurança da informação?
17. A organização possui um ponto de contato para notificação e registro de quaisquer fragilidades de segurança da informação observada ou suspeita?
18. A organização estabelece, documenta, implementa e mantém processos, procedimentos e controles para assegurar o nível requerido de continuidade para a segurança da informação durante uma situação adversa?
19. São implementados recursos de processamento da informação com redundância suficiente para atender aos requisitos de disponibilidade?