****

**LISTA DE VERIFICAÇÃO DE CONTINUIDADE DE NEGÓCIOS DAD ISO 27001**

|  |  |  |  |
| --- | --- | --- | --- |
| **SEÇÃO DE REQUISITOS/****CATEGORIA** | **AVALIAÇÃO** | **EM CONFORMIDADE?** | **OBSERVAÇÕES** |
| ***5. Políticas de segurança da informação*** |  |  |
| 5.1 | Há políticas de segurança? |   |  |
| 5.2 | Todas as políticas são aprovadas pelo gerenciamento? |   |  |
| 5.3 | Evidência de conformidade? |   |  |
| ***6. Organização de segurança da informação*** |   |  |
| 6.1 | Funções e responsabilidades definidas? |   |  |
| 6.2 | Segregação de tarefas definidas? |   |  |
| 6.3 | Órgão/autoridade de verificação contatada para verificação da conformidade? |   |  |
| 6.4 | Contato estabelecido com grupos de interesse especial relacionados à conformidade? |   |  |
| 6.5 | Evidência de segurança da informação no gerenciamento de projeto? |   |  |
| 6.6 | Política definida para trabalhar remotamente? |   |  |
| ***7. Segurança dos recursos humanos*** |   |  |
| 7.1 | Política definida para seleção de funcionários antes da contratação? |   |  |
| 7.2 | Política definida para os termos e condições do RH para contratação? |   |  |
| 7.3 | Política definida para as responsabilidades do gerenciamento? |   |  |
| 7.4 | Política definida para conscientização, educação e treinamento em segurança da informação? |   |  |
| 7.5 | Política definida para processo disciplinar com relação à segurança da informação? |   |  |
| 7.6 | Política definida para rescisão do RH ou para mudança de emprego com relação à segurança da informação? |   |  |
| ***8. Gerenciamento de ativos*** |   |  |
| 8.1 | Lista completa de inventário de ativos? |   |  |
| 8.2 | Lista completa de propriedade de ativos? |   |  |
| 8.3 | Política definida para "uso aceitável" de ativos? |   |  |
| 8.4 | Política definida de devolução de ativos? |   |  |
| 8.5 | Política definida para classificação de informações? |   |  |
| 8.6 | Política definida para rotular informações? |   |  |
| 8.7 | Política definida para manipulação de ativos? |   |  |
| 8.8 | Política definida para gerenciamento de mídia removível? |   |  |
| 8.9 | Política definida para descarte de mídia? |   |  |
| 8.10 | Política definida para transferência de mídia física? |   |  |
| ***9. Controle de acesso***  |   |  |
| 9.1 | Política definida para controle de acesso? |   |  |
| 9.2 | Política definida para acesso a redes e serviços de rede? |   |  |
| 9.3 | Política definida para registro e cancelamento de registro de ativos de usuário? |   |  |
| 9.4 | Política definida para provisionamento de acesso ao usuário? |   |  |
| 9.5 | Política definida para gerenciamento de direitos de acesso privilegiado? |   |  |
| 9.6 | Política definida para gerenciamento de autenticação secreta de informações dos usuários? |   |  |
| 9.7 | Política definida para revisão dos direitos de acesso de usuário? |   |  |
| 9.8 | Política definida para remoção ou ajuste de direitos de acesso? |   |  |
| 9.9 | Política definida para uso de informações de autenticação secreta? |   |  |
| 9.10 | Política definida para restrições de acesso às informações? |   |  |
| 9.11 | Política definida para procedimentos de login seguro? |   |  |
| 9.12 | Política definida para sistemas de gerenciamento de senhas? |   |  |
| 9.13 | Política definida para uso de programas utilitários privilegiados? |   |  |
| 9.14 | Política definida para controle de acesso ao código-fonte do programa? |   |  |
| ***10. Criptografia*** |   |  |
| 10.1 | Política definida para uso de controles criptográficos? |   |  |
| 10.2 | Política definida para gerenciamento de chaves? |   |  |
| ***11. Segurança física e ambiental*** |   |  |
| 11.1 | Política definida para perímetro de segurança física? |   |  |
| 11.2 | Política definida para controles de entrada física? |   |  |
| 11.3 | Política definida para proteção de escritórios, salas e instalações? |   |  |
| 11.4 | Política definida para proteção contra ameaças externas e ambientais? |   |  |
| 11.5 | Política definida para trabalhar em áreas seguras? |   |  |
| 11.6 | Política definida para áreas de carga e descarga? |   |  |
| 11.7 | Política definida para localização e proteção de equipamentos? |   |  |
| 11.8 | Política definida para utilitários de suporte? |   |  |
| 11.9 | Política definida para segurança do cabeamento? |   |  |
| 11.10 | Política definida para manutenção de equipamentos? |   |  |
| 11.11 | Política definida para remoção de ativos? |   |  |
| 11.12 | Política definida para segurança de equipamento e ativos fora das instalações? |   |  |
| 11.13 | Descarte seguro ou reutilização de equipamentos? |   |  |
| 11.14 | Política definida para equipamento do usuário sem supervisão? |   |  |
| 11.15 | Política definida para escrivaninha e tela limpas? |   |  |
| ***12. Segurança das operações*** |   |  |
| 12.1 | Política definida para procedimentos de operação documentados? |   |  |
| 12.2 | Política definida para gerenciamento de mudanças? |   |  |
| 12.3 | Política definida para gerenciamento de capacidade? |   |  |
| 12.4 | Política definida para separação de ambientes de desenvolvimento, testes e operações? |   |  |
| 12.5 | Política definida para controles contra malware? |   |  |
| 12.6 | Política definida para backup de sistemas? |   |  |
| 12.7 | Política definida para backup de informações? |   |  |
| 12.8 | Política definida para registro de eventos? |   |  |
| 12.9 | Política definida para proteção de informações de registros? |   |  |
| 12.10 | Política definida para registro do administrador e do operador? |   |  |
| 12.11 | Política definida para sincronização de relógios? |   |  |
| 12.12 | Política definida para instalação de software em sistemas operacionais? |   |  |
| 12.13 | Política definida para gerenciamento de vulnerabilidades técnicas? |   |  |
| 12.14 | Política definida para restrição à instalação de software? |   |  |
| 12.15 | Política definida para controle de auditoria de sistemas da informação? |   |  |
| ***13. Segurança das comunicações*** |   |  |
| 13.1 | Política definida para controles de rede? |   |  |
| 13.2 | Política definida para segurança dos serviços da rede? |   |  |
| 13.3 | Política definida para segregação em redes? |   |  |
| 13.4 | Política definida para procedimentos e políticas de transferência de informações? |   |  |
| 13.5 | Política definida para contratos de transferência de informações? |   |  |
| 13.6 | Política definida para mensagens eletrônicas? |   |  |
| 13.7 | Política definida para contratos de confidencialidade ou não divulgação? |   |  |
| 13.8 | Política definida para aquisição, desenvolvimento e manutenção de sistemas? |   |  |
| ***14. Aquisição, desenvolvimento e manutenção de sistemas***  |
| 14.1 | Política definida para análise e especificação de requisitos de segurança da informação? |   |  |
| 14.2 | Política definida para proteção de serviços de aplicativos em redes públicas? |   |  |
| 14.3 | Política definida para proteção de transações de serviço de aplicativo? |   |  |
| 14.4 | Política definida para desenvolvimento interno? |   |  |
| ***15. Relacionamentos com fornecedores*** |   |  |
| 15.1 | Política definida para relacionamentos com fornecedores? |   |  |
| ***16. Gerenciamento de incidentes de segurança da informação*** |
| 16.1 | Política definida para gerenciamento de segurança da informação? |   |  |
| ***17. Aspectos de segurança da informação no gerenciamento da continuidade dos negócios*** |
| 17.1 | Política definida para continuidade da segurança da informação? |   |  |
| 17.2 | Política definida para redundâncias? |   |  |
| ***18. Conformidade*** |   |  |
| 18.1 | Política definida para identificação dos requisitos legais e contratuais aplicáveis? |   |  |
| 18.2 | Política definida para direitos de propriedade intelectual? |   |  |
| 18.3 | Política definida para proteção de registros? |   |  |
| 18.4 | Política definida para privacidade e proteção de dados pessoais identificáveis? |   |  |
| 18.5 | Política definida para regulamentação do controle criptográfico? |   |  |
| 18.6 | Política definida para conformidade com as políticas e normas de segurança? |   |  |
| 18.7 | Política definida para revisão da conformidade técnica? |   |  |

**AVISO DE ISENÇÃO DE RESPONSABILIDADE**

Qualquer artigo, modelo ou informação fornecidos pela Smartsheet no site são apenas para referência. Embora nos esforcemos para manter as informações atualizadas e corretas, não fornecemos garantia de qualquer natureza, seja explícita ou implícita, a respeito da integridade, precisão, confiabilidade, adequação ou disponibilidade do site ou das informações, artigos, modelos ou gráficos contidos no site. Portanto, toda confiança que você depositar nessas informações será estritamente por sua própria conta e risco.

Este modelo é fornecido apenas como amostra. Este modelo não é, de forma alguma, conselho jurídico ou de conformidade. Os usuários deste modelo devem determinar quais informações são necessárias para alcançar seus objetivos.