CONTROLES
ISO 27002:2012

A.5 CONTROLES ORGANIZACIONAIS

5.1 - Políticas para Segurança da Informação
5.2 - Funções e Responsabilidades de Segurança da Informação
5.3 - Segregação de Funções
5.4 - Responsabilidades da Gestão
5.5 - Contato com as autoridades
5.6 - Contato com grupos de interesse específicos
5.7 - Threat intelligence
5.8 - Segurança da informação no gerenciamento de projetos
5.9 - Inventário de informações e outros ativos associados
5.10 - Uso aceitável de informações e outros ativos associados
5.11 - Retorno de Ativos
5.12 - Classificação da Informação
5.13 - Rotulagem da Informação
5.14 - Transferência da Informação
5.15 - Controle de Acesso
5.16 - Gerenciamento de identidades
5.17 - Autenticação
5.18 - Direitos de Acesso
5.19 - Segurança da informação nos relacionamentos com fornecedores
5.20 - Endereçando a segurança da informação dentro dos contratos com fornecedores
5.21 - Gerenciando a segurança da informação na cadeia de suprimentos de TIC
5.22 - Monitoramento, revisão e alteração de gerenciamento de serviços de fornecedores
5.23 - Segurança da informação para uso de serviços de nuvem
5.24 - Planejamento e preparação de gerenciamento de incidentes de segurança da informação
5.25 - Avaliação e decisão sobre eventos de segurança da informação
5.26 - Resposta aos incidentes de segurança da informação
5.27 - Aprendizado com incidentes de segurança da informação
5.28 - Coleta de evidências
5.29 - Segurança da Informação durante interrupções
5.30 - Prontidão de TI para Continuidade de Negócios
5.31 - Identificação de requisitos legais, estatutários, regulamentares e contratuais
5.32 - Direitos de propriedade intelectual
5.33 - Proteção de registros
5.34 - Privacidade e proteção de dados PII
5.35 - Revisão independente da segurança da informação
5.36 - Conformidade com políticas e padrões para segurança da informação
5.37 - Documentação de Procedimentos Operacionais

A.6 CONTROLES DE PESSOAS

6.1 - Triagem
6.2 - Termos e Condições de Emprego
6.3 - Conscientização de segurança da informação, educação e treinamento
6.4 - Processo Disciplinar
6.5 - Responsabilidades após rescisão ou mudança de emprego
6.6 - Contratos de confidencialidade ou não divulgação
6.7 - Trabalho Remoto
6.8 - Relatórios de eventos de segurança da informação

A.7 CONTROLES FÍSICOS

7.1 - Segurança física de perímetro
7.2 - Controles de entrada física
7.3 - Protegendo escritório, salas e instalações
7.4 - Monitoramento de segurança física
7.5 - Protegendo contra ameaças físicas e ambientais
7.6 - Trabalhando em áreas seguras
7.7 - Mesa e Tela Limpa
7.8 - Localização e proteção de equipamentos
7.9 - Segurança de ativos fora do local de trabalho
7.10 - Mídia de armazenamento
7.11 - Utilitários de suporte
7.12 - Segurança de cabeamento
7.13 - Manutenção de equipamentos
7.14 - Descarte seguro ou reutilização de equipamentos

A.8 CONTROLES TÉCNICOS

8.1 - Dispositivos de endpoint
8.2 - Direitos de acesso privilegiado
8.3 - Restrição de acesso à informação
8.4 - Acesso ao código-fonte
8.5 - Autenticação segura
8.6 - Gerenciamento de Capacidade
8.7 - Proteção contra malware
8.8 - Gestão de vulnerabilidades técnicas
8.9 - Gerenciamento de Configuração
8.10 - Exclusão de informações
8.11 - Mascaramento de dados
8.12 - Prevenção de vazamento de dados
8.13 - Backup de informações
8.14 - Redundância de instalações de processamento de informações
8.15 - Registro de logs
8.16 - Atividades de monitoramento
8.17 - Sincronização do relógio
8.18 - Uso de programas utilitários e privilegiados
8.19 - Instalação de software em sistemas operacionais
8.20 - Controles de rede
8.21 - Segurança de serviços de rede
8.22 - Filtragem da Web
8.23 - Segregação em redes
8.24 - Uso de criptografia
8.25 - Ciclo de vida de desenvolvimento seguro
8.26 - Requisitos de segurança de aplicativos
8.27 - Princípios seguros de arquitetura e engenharia do sistema
8.28 - Codificação segura
8.29 - Testes de segurança em desenvolvimento e aceitação
8.30 - Desenvolvimento terceirizado
8.31 - Separação de ambientes de desenvolvimento, teste e produção
8.32 - Gerenciamento de Mudanças
8.33 - Informações sobre testes
8.34 - Proteção de sistemas de informação durante a auditoria e testes