CONTROLES
ISO27001:2013

A.5 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

5.1.1 - Políticas para Segurança da Informação
5.1.2 - Funções e Responsabilidades de Segurança da Informação

A.6 ORGANIZAÇÃO DA SEGURANÇA DA INFORMAÇÃO

6.1.1 - Responsabilidade e papéis pela segurança da informação
6.1.2 - Segregação de função
6.1.3 - Contato com Autoridades
6.1.4 - Contato com Grupos Especiais
6.1.5 - Segurança da Informação no Gerenciamento de Projetos
6.2.1 - Política para o uso de dispositivo móvel
6.2.2 - Trabalho Remoto

A.7 SEGURANÇA EM RECURSOS HUMANOS

7.1.1 - Seleção
7.1.2 - Termos e Condições de Contratação
7.2.1 - Responsabilidades da Direção
7.2.2 - Conscientização, educação e treinamento em segurança da informação.
7.2.3 - Processo Disciplinar
7.3.1 - Responsabilidades pelo encerramento ou mudança da contratação

A.8 GESTÃO DE ATIVOS

8.1.1 - Inventário dos Ativos
8.1.2 - Proprietário dos ativos
8.1.3 - Uso aceitável dos ativos
8.1.4 - Devolução de ativos
8.2.1 - Classificação da informação
8.2.2 - Rótulos e Tratamento da Informação
8.2.3 - Tratamento dos ativos
8.3.1 - Gerenciamento de mídias removíveis
8.3.2 - Descarte de mídias
8.3.3 - Transferência física de mídias

A.9 CONTROLE DE ACESSO

9.1.1 - Política de controle de acesso
9.1.2 - Acesso às redes e aos serviços de rede
9.2.1 - Registro e cancelamento de usuário
9.2.2 - Provisionamento para acesso de usuário
9.2.3 - Gerenciamento de direitos de acesso privilegiado
9.2.4 - Gerenciamento da informação de autenticação secreta de usuários
9.2.5 - Análise crítica dos direitos de acesso de usuário
9.2.6 - Retirada ou ajuste dos direitos de acesso
9.3.1 - Uso de informação de autenticação secreta
9.4.1 - Restrição de acesso à informação
9.4.2 - Procedimentos seguros de entrada no sistema (log-on)
9.4.3 - Sistema de gerenciamento de senhas
9.4.4 - Uso de programas utilitários e privilegiados
9.4.5 - Controles de acesso ao código fonte de programas

A.10 CRIPTOGRAFIA

10.1.1 - Política para o uso de controles criptográficos
10.1.2 - Gerenciamento de Chaves

A.11 SEGURANÇA FÍSICA E DO AMBIENTE

11.1.1 - Perímetro de Segurança Física
11.1.2 - Controles de Entrada Física
11.1.3 - Segurança em escritórios, salas e instalações
11.1.4 - Proteção contra ameaças externas e do meio ambiente
11.1.5 - Trabalhando em áreas seguras
11.1.6 - Áreas de entrega e de carregamento
11.2.1 - Localização e proteção do equipamento
11.2.2 - Utilidades
11.2.3 - Segurança do Cabeamento
11.2.4 - Manutenção dos Equipamentos
11.2.5 - Remoção de ativos
11.2.6 - Segurança de equipamentos fora das dependências da organização
11.2.7 - Reutilização ou descarte seguro de equipamentos
11.2.8 - Equipamento de usuário sem monitoração
11.2.9 - Política de mesa limpa e tela limpa

A.12 SEGURANÇA NAS OPERAÇÕES

12.1.1 - Documentação dos procedimentos de operação
12.1.2 - Gestão de Mudanças
12.1.3 - Gestão de capacidade
12.1.4 - Separação dos recursos de desenvolvimento, teste e de produção
12.2.1 - Controle contra malware
12.3.1 - Cópias de Segurança das Informações
12.4.1 - Registros de eventos
12.4.2 - Proteção das informações dos registros de eventos (logs)
12.4.3 - Registros de eventos (log) de administrador e operador
12.4.4 - Sincronização dos relógios
12.5.1 - Instalação de software nos sistemas operacionais
12.6.1 - Gestão de vulnerabilidades técnicas
12.6.2 - Restrição quanto a instalação de software
12.7.1 - Controles de auditoria de sistemas de informação

A.13 SEGURANÇA NAS COMUNICAÇÕES

13.1.1 - Controles de redes
13.1.2 - Segurança dos serviços de rede
13.1.3 - Segregação de redes
13.2.1 - Políticas e procedimentos para transferência de Informações
13.2.2 - Acordos para a transferência de Informações
13.2.3 - Mensagens eletrônicas
13.2.4 - Acordos de confidencialidade e não divulgação

A.14 AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS

14.1.1 - Analise e especificações dos requisitos de segurança da informação
14.1.2 - Serviços de aplicação seguros em redes públicas
14.1.3 - Protegendo as transações nos aplicativos de serviços
14.2.1 - Política de desenvolvimento seguro
14.2.2 - Procedimento para controle de mudança de sistemas
14.2.3 - Análise crítica técnica das aplicações após mudanças nas plataformas operacionais
14.2.4 - Restrições sobre mudanças em pacotes de software
14.2.5 - Princípios para projetar sistemas seguros
14.2.6 - Ambiente seguro para desenvolvimento
14.2.7 - Desenvolvimento terceirizado
14.2.8 - Teste de segurança do sistema
14.2.9 - Teste de aceitação de sistemas
14.3.1 - Proteção dos dados para teste

A.15 RELACIONAMENTO NA CADEIA DE SUPRIMENTOS

15.1.1 - Política de Segurança da Informação no relacionamento com os fornecedores
15.1.2 - Identificando segurança da informação nos acordos com fornecedores
15.1.3 - Cadeia de suprimento na tecnologia da informação e comunicação
15.2.1 - Monitoramento e análise crítica de serviços com fornecedores
15.2.2 - Gerenciamento de mudanças para serviços com fornecedores

A.16 GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

16.1.1 - Responsabilidades e procedimentos
16.1.2 - Notificação de eventos de segurança da informação
16.1.3 - Notificando fragilidades de segurança da informação
16.1.4 - Avaliação e decisão dos eventos de segurança da informação.
16.1.5 - Respostas a incidentes de segurança da informação
16.1.6 - Aprendendo com os incidentes de segurança da informação
16.1.7 - Coleta de evidências

A.17 ASPECTOS DA SEGURANÇA DA INFORMAÇÃO NA GESTÃO DA CONTINUIDADE DO NEGÓCIO

17.1.1 - Planejamento a continuidade da segurança da informação
17.1.2 - Implementando a continuidade da segurança da informação
17.1.3 - Verificação, análise crítica e avaliação da continuidade da segurança da informação
17.2.1 - Disponibilidade dos recursos de processamento da informação

A.18 CONFORMIDADE

18.1.1 - Identificação da legislação aplicável e de requisitos contratuais
18.1.2 - Direitos de propriedade intelectual
18.1.3 - Proteção de registros
18.1.4 - Proteção e privacidade de informações de identificação de pessoal
18.1.5 - Regulamentação de controles de criptografia
18.2.1 - Análise crítica independente da segurança da informação
18.2.2 - Conformidade com as políticas e normas de segurança da informação
18.2.3 - Análise crítica da conformidade técnica