Formulário para avaliação do nível de maturidade da segurança da informação

Seção	Categoria	Controles	Descrição	Nível de Maturidade atual		Nível de Maturidade Objetivo		Avaliador(es)	Data da última avaliação	Processos e atividades relacionadas	Planos de Ação Sugeridos
5			**Política de segurança da informação**								
5	**1**		**Política de segurança da informação**								
5	1	1	Documento da política de segurança da informação								
5	1	2	Análise crítica da política de segurança da informação								
6			**Organizando a segurança da informação**								
6	**1**		**Organização interna**								
6	1	1	Comprometimento da organização com a segurança da informação								
6	1	2	Coordenação da segurança da informação								
6	1	3	Atribuição de responsabilidades para a segurança da informação								
6	1	4	Processo de autorização para os recursos de processamento da informação								
6	1	5	Acordos de confidencialidade								
6	1	6	Contato com autoridades								
6	1	7	Contato com grupos especiais								
6	1	8	Análise crítica independente da segurança da informação								
6	**2**		**Partes externas**								
6	2	1	Identificação dos riscos relacionados com partes externas								
6	2	2	Identificando a segurança da informação, quando tratando com os clientes								
6	2	3	Identificando segurança da informação nos acordos com terceiros								
7			**Gestão de ativos**								
7	**1**		**Responsabilidade pelos ativos**								
7	1	1	Inventário dos ativos								
7	1	2	Proprietário dos ativos								
7	1	3	Uso aceitável dos ativos								
7	**2**		**Classificação da informação**								
7	2	1	Recomendações para classificação								
7	2	2	Rótulos e tratamento da informação								
8			**Segurança em recursos humanos**								
8	**1**		**Antes da contratação**								
8	1	1	Papéis e responsabilidades								
8	1	2	Seleção								
8	1	3	Termos e condições de contratação								
8	**2**		**Durante a contratação**								
8	2	1	Responsabilidades da direção								

Seção	Categoria	Controles	Descrição	Nível de Maturidade atual		Nível de Maturidade Objetivo		Avaliador(es)	Data da última avaliação	Processos e atividades relacionadas	Planos de Ação Sugeridos
8	2	2	Conscientização, educação e treinamento em segurança da informação								
8	2	3	Processo disciplinar								
8	**3**		**Encerramento ou mudança da contratação**								
8	3	1	Encerramento de atividades								
8	3	2	Devolução de ativos								
8	3	3	Retirada de direitos de acesso								
9			**Segurança física e do ambiente**								
9	**1**		**Áreas seguras**								
9	1	1	Perímetro de segurança física								
9	1	2	Controles de entrada física								
9	1	3	Segurança em escritórios, salas e instalações								
9	1	4	Proteção contra ameaças externas e do meio ambiente								
9	1	5	Trabalhando em áreas seguras								
9	1	6	Acesso do público, áreas de entrega e de carregamento								
9	**2**		**Segurança de equipamentos**								
9	2	1	Instalação e proteção do equipamento								
9	2	2	Utilidades								
9	2	3	Segurança do cabeamento								
9	2	4	Manutenção dos equipamentos								
9	2	5	Segurança de equipamentos fora das dependências da organização								
9	2	6	Reutilização e alienação segura de equipamentos								
9	2	7	Remoção da propriedade								
10			**Gerenciamento das operações e comunicações**								
10	**1**		**Procedimentos e responsabilidades operacionais**								
10	1	1	Documentação dos procedimentos de operação								
10	1	2	Gestão de mudanças								
10	1	3	Segregação de funções								
10	1	4	Separação dos recursos de desenvolvimento, teste e de produção								
10	**2**		**Gerenciamento de serviços terceirizados**								
10	2	1	Entrega de serviços								
10	2	2	Monitoramento e análise crítica de serviços terceirizados								
10	2	3	Gerenciamento de mudanças para serviços terceirizados								
10	**3**		**Planejamento e aceitação dos sistemas**								
10	3	1	Gestão de capacidade								
10	3	2	Aceitação de sistemas								
10	**4**		**Proteção contra códigos maliciosos e códigos móveis**								
10	4	1	Controles contra códigos maliciosos								
10	4	2	Controles contra códigos móveis								
10	**5**		**Cópias de segurança**								
10	5	1	Cópias de segurança das informações								

Seção	Categoria	Controles	Descrição	Nível de Maturidade atual		Nível de Maturidade Objetivo		Avaliador(es)	Data da última avaliação	Processos e atividades relacionadas	Planos de Ação Sugeridos
10	**6**		**Gerenciamento da segurança em redes**								
10	6	1	Controles de redes								
10	6	2	Segurança dos serviços de rede								
10	**7**		**Manuseio de mídias**								
10	7	1	Gerenciamento de mídias removíveis								
10	7	2	Descarte de mídias								
10	7	3	Procedimentos para tratamento de informação								
10	7	4	Segurança da documentação dos sistemas								
10	**8**		**Troca de informações**								
10	8	1	Políticas e procedimentos para troca de informações								
10	8	2	Acordos para troca de informações								
10	8	3	Mídias em trânsito								
10	8	4	Mensagens eletrônicas								
10	8	5	Sistemas de informações de negócios								
10	**9**		**Serviços de comércio eletrônico**								
10	9	1	Comércio eletrônico								
10	9	2	Transações online								
10	9	3	Informações publicamente disponíveis								
10	**10**		**Monitoramento**								
10	10	1	Registros de auditoria								
10	10	2	Monitoramento do uso do sistema								
10	10	3	Proteção das informações dos registros (log)								
10	10	4	Registros (log) de administrador e operador								
10	10	5	Registros (log) de falhas								
10	10	6	Sincronização dos relógios								
11			**Controle de acessos**								
11	**1**		**Requisitos de negócio para controle de acesso**								
11	1	1	Política de controle de acesso								
11	**2**		**Gerenciamento de acesso do usuário**								
11	2	1	Registro de usuário								
11	2	2	Gerenciamento de privilégios								
11	2	3	Gerenciamento de senha do usuário								
11	2	4	Análise crítica dos direitos de acesso de usuário								
11	**3**		**Responsabilidades dos usuários**								
11	3	1	Uso de senhas								
11	3	2	Equipamento de usuário sem monitoração								
11	3	3	Política de mesa limpa e tela limpa								
11	**4**		**Controle de acesso à rede**								
11	4	1	Política de uso dos serviços de rede								
11	4	2	Autenticação para conexão externa do usuário								
11	4	3	Identificação de equipamentos em redes								

Seção	Categoria	Controles	Descrição	Nível de Maturidade atual		Nível de Maturidade Objetivo		Avaliador(es)	Data da última avaliação	Processos e atividades relacionadas	Planos de Ação Sugeridos
11	4	4	Proteção de portas de configuração e diagnóstico remotos								
11	4	5	Segregação de redes								
11	4	6	Controle de conexão de rede								
11	4	7	Controle de roteamento de redes								
11	**5**		**Controle de acesso ao sistema operacional**								
11	5	1	Procedimentos seguros de entrada no sistema (log-on)								
11	5	2	Identificação e autenticação de usuário								
11	5	3	Sistema de gerenciamento de senha								
11	5	4	Uso de utilitários de sistema								
11	5	5	Limite de tempo de conexão								
11	5	6	Limitação de horário de conexão								
11	**6**		**Controle de acesso à aplicação e à informação**								
11	6	1	Restrição de acesso à informação								
11	6	2	Isolamento de sistemas sensíveis								
11	**7**		**Comutação móvel e trabalho remoto**								
11	7	1	Computação e comunicação móvel								
11	7	2	Trabalho remoto								
12			**Aquisição, desenvolvimento e manutenção de sistemas de informação**								
12	**1**		**Requisitos de segurança de sistemas de informação**								
12	1	1	Análise e especificação dos requisitos de segurança								
12	**2**		**Processamento correto nas aplicações**								
12	2	1	Validação dos dados de entrada								
12	2	2	Controle do processamento interno								
12	2	3	Integridade de mensagens								
12	2	4	Validação dos dados de saída								
12	**3**		**Controles criptográficos**								
12	3	1	Política para o uso de controles criptográficos								
12	3	2	Gerenciamento de chaves								
12	**4**		**Segurança dos arquivos do sistema**								
12	4	1	Controle de software operacional								
12	4	2	Proteção dos dados para teste de sistema								
12	4	3	Controle de acesso ao código-fonte de programa								
12	**5**		**Segurança em processos de desenvolvimento e suporte**								
12	5	1	Procedimentos para controle de mudanças								
12	5	2	Análise crítica técnica das aplicações após mudanças no sistema operacional								
12	5	3	Restrições sobre mudanças em pacotes de software								
12	5	4	Vazamento de informações								
12	5	5	Desenvolvimento terceirizado de software								
12	**6**		**Gestão de vulnerabilidades técnicas**								

Seção	Categoria	Controles	Descrição	Nível de Maturidade atual		Nível de Maturidade Objetivo		Avaliador(es)	Data da última avaliação	Processos e atividades relacionadas	Planos de Ação Sugeridos
12	6	1	Controle de vulnerabilidades técnicas								
13			**Gestão de incidentes de segurança da informação**								
13	**1**		**Notificação de fragilidades e eventos de segurança da informação**								
13	1	1	Notificação de eventos de segurança da informação								
13	1	2	Notificação de fragilidades de segurança da informação								
13	**2**		**Gestão de incidentes de segurança da informação e melhorias**								
13	2	1	Responsabilidades e procedimentos								
13	2	2	Aprendendo com os incidentes de segurança da informação								
13	2	3	Coleta de evidências								
14			**Gestão da continuidade do negócio**								
14	**1**		**Aspectos da continuidade do negócio, relativos à segurança da informação**								
14	1	1	Incluindo segurança da informação no processo de gestão da continuidade do negócio								
14	1	2	Continuidade de negócios e análise/avaliação de riscos								
14	1	3	Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação								
14	1	4	Estrutura do plano de continuidade do negócio								
14	1	5	Testes, manutenção e reavaliação dos planos de continuidade do negócio								
15			**Conformidade**								
15	**1**		**Conformidade com requisitos legais**								
15	1	1	Identificação da legislação aplicável								
15	1	2	Direitos de propriedade intelectual								
15	1	3	Proteção de registros organizacionais								
15	1	4	Proteção de dados e privacidade de informações pessoais								
15	1	5	Prevenção de mau uso de recursos de processamento da informação								
15	1	6	Regulamentação de controles de criptografia								
15	**2**		**Conformidade com normas e políticas de segurança da informação e conformidade técnica**								
15	2	1	Conformidade com as políticas e normas de segurança da informação								
15	2	2	Verificação da conformidade técnica								
15	**3**		**Considerações quanto à auditoria de sistemas de informação**								
15	3	1	Controles de auditoria de sistemas de informação								
15	3	2	Proteção de ferramentas de auditoria de sistemas de informação								